Sun Java System Application Server 9.1 Reference Manual



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

Part No: 819–3675–10 Sptember 2007 Copyright 2007 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

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

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

This distribution may include materials developed by third parties.

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

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

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

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

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

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

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

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

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

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

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

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

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

Contents

Preface	11
Application Server 9.1 Section 1: Administration Commands	
add-resources(1)	14
apply-http-lb-changes(1)	
backup-domain(1)	20
change-admin-password(1)	22
change-master-password(1)	23
clear-ha-store(1)	25
configure-ha-cluster(1)	28
configure-ha-persistence(1)	
configure-lb-weight(1)	37
configure-webservice-management(1)	40
copy-config(1)	43
create-admin-object(1)	46
create-application-ref(1)	49
create-audit-module(1)	52
create-auth-realm(1)	55
create-cluster(1)	58
create-connector-connection-pool(1)	63
create-connector-resource(1)	67
create-connector-security-map(1)	70
create-custom-resource(1)	73
create-domain(1)	76
create-file-user(1)	82
create-ha-store(1)	85
create-http-health-checker(1)	88
create-http-lb(1)	91

create-http-lb-config(1)	96
create-http-lb-ref(1)	100
create-http-listener(1)	105
create-iiop-listener(1)	109
create-instance(1)	112
create-javamail-resource(1)	117
create-jdbc-connection-pool(1)	121
create-jdbc-resource(1)	126
create-jmsdest(1)	129
create-jms-host(1)	132
create-jms-resource(1)	135
create-jndi-resource(1)	141
create-jvm-options(1)	145
create-lifecycle-module(1)	148
create-management-rule(1)	151
create-mbean(1)	159
create-message-security-provider(1)	163
create-node-agent(1)	167
create-node-agent-config(1)	170
create-password-alias(1)	173
create-persistence-resource(1)	
create-profiler(1)	180
create-resource-adapter-config(1)	183
create-resource-ref(1)	186
create-service(1)	189
create-ssl(1)	191
create-system-properties(1)	195
create-threadpool(1)	197
create-transformation-rule(1)	200
create-virtual-server(1)	203
delete-admin-object(1)	210
delete-application-ref(1)	213
delete-audit-module(1)	216
delete-auth-realm(1)	219
delete-cluster(1)	222
delete-config(1)	225

delete-connector-connection-pool(1)	227
delete-connector-resource(1)	230
delete-connector-security-map(1)	233
delete-custom-resource(1)	236
delete-domain(1)	239
delete-file-user(1)	240
delete-http-health-checker(1)	243
delete-http-lb(1)	246
delete-http-lb-config(1)	248
delete-http-lb-ref(1)	251
delete-http-listener(1)	254
delete-iiop-listener(1)	257
delete-instance(1)	260
delete-javamail-resource(1)	262
delete-jdbc-connection-pool(1)	265
delete-jdbc-resource(1)	268
delete-jmsdest(1)	271
delete-jms-host(1)	274
delete-jms-resource(1)	277
delete-jndi-resource(1)	280
delete-jvm-options(1)	283
delete-lifecycle-module(1)	286
delete-management-rule(1)	289
delete-mbean(1)	292
delete-message-security-provider(1)	295
delete-node-agent(1)	298
delete-node-agent-config(1)	299
delete-password-alias(1)	302
delete-persistence-resource(1)	304
delete-profiler(1)	307
delete-resource-adapter-config(1)	310
delete-resource-ref(1)	313
delete-ssl(1)	316
delete-system-property(1)	319
delete-threadpool(1)	321
delete-transformation-rule(1)	324

delete-virtual-server(1)	327
deploy(1)	
deploydir(1)	336
deploy-jbi-service-assembly(1)	342
disable(1)	345
disable-http-lb-application(1)	348
disable-http-lb-server(1)	351
display-error-distribution(1)	354
display-error-statistics(1)	357
display-license(1)	360
display-log-records(1)	363
enable(1)	367
enable-http-lb-application(1)	370
enable-http-lb-server(1)	373
export(1)	376
export-http-lb-config(1)	377
flush-jmsdest(1)	381
freeze-transaction-service(1)	384
generate-diagnostic-report(1)	387
generate-jvm-report(1)	
get(1)	394
get-client-stubs(1)	411
get-health(1)	414
help(1)	416
install-jbi-component(1)	430
install-jbi-shared-library(1)	434
install-license(1)	437
jms-ping(1)	438
list(1)	441
list-acls(1)	454
list-admin-objects(1)	455
list-application-refs(1)	458
list-audit-modules(1)	461
list-auth-realms(1)	464
list-backups(1)	467
list-clusters(1)	468

list-components(1)	471
list-configs(1)	474
list-connector-connection-pools(1)	477
list-connector-resources(1)	479
list-connector-security-maps(1)	482
list-custom-resources(1)	485
list-domains(1)	488
list-file-groups(1)	489
list-file-users(1)	492
list-http-lb-configs(1)	495
list-http-lbs(1)	498
list-http-listeners(1)	501
list-iiop-listeners(1)	504
list-instances(1)	507
list-javamail-resources(1)	509
list-jbi-binding-components(1)	512
list-jbi-service-assemblies(1)	515
list-jbi-service-engines(1)	518
list-jbi-shared-libraries(1)	521
list-jdbc-connection-pools(1)	524
list-jdbc-resources(1)	526
list-jmsdest(1)	529
list-jms-hosts(1)	532
list-jms-resources(1)	535
list-jndi-entries(1)	538
list-jndi-resources(1)	541
list-lifecycle-modules(1)	544
list-management-rules(1)	547
list-mbeans(1)	549
list-message-security-providers(1)	552
list-node-agents(1)	555
list-password-aliases(1)	558
list-persistence-resources(1)	560
list-registry-locations(1)	563
list-resource-adapter-configs(1)	565
list-resource-refs(1)	568

list-sub-components(1)	571
list-system-properties(1)	573
list-threadpools(1)	576
list-timers(1)	579
list-transformation-rules(1)	582
list-virtual-servers(1)	584
login(1)	587
migrate-timers(1)	590
monitor(1)	593
multimode(1)	598
ping-connection-pool(1)	599
publish-to-registry(1)	602
recover-transactions(1)	605
remove-ha-cluster(1)	608
restore-domain(1)	611
rollback-transaction(1)	613
set(1)	615
show-component-status(1)	626
show-jbi-binding-component(1)	629
show-jbi-service-assembly(1)	632
show-jbi-service-engine(1)	635
show-jbi-shared-library(1)	638
shutdown(1)	641
shut-down-jbi-component(1)	642
shut-down-jbi-service-assembly(1)	645
start-appserv(1)	648
start-callflow-monitoring(1)	650
start-cluster(1)	653
start-database(1)	656
start-domain(1)	658
start-instance(1)	660
start-jbi-component(1)	663
start-jbi-service-assembly(1)	666
start-node-agent(1)	669
stop-appserv(1)	672
stop-callflow-monitoring(1)	673

stop-cluster(1)	676
stop-database(1)	679
stop-domain(1)	680
stop-instance(1)	681
stop-jbi-component(1)	684
stop-jbi-service-assembly(1)	687
stop-node-agent(1)	690
undeploy(1)	691
undeploy-jbi-service-assembly(1)	695
unfreeze-transaction-service(1)	698
uninstall-jbi-component(1)	701
uninstall-jbi-shared-library(1)	704
unpublish-from-registry(1)	707
unset(1)	709
update-connector-security-map(1)	710
update-file-user(1)	713
update-password-alias(1)	716
verify-domain-xml(1)	719
version(1)	720
Application Server 9.1 Section 1M: Utility Commands	72.3
appclient(1M)	
asadmin(1M)	
asant(1M)	
asmigrate(1m)	
asupgrade(1M)	
capture-schema(1m)	
deploytool(1m)	
jspc(1M)	
package-appclient(1M)	
schemagen(1M)	
updatetool(1m)	
verifier(1M)	
wscompile(1M)	
wsdeploy(1M)	
± / ` /	

wsgen(1M)	
wsimport(1M)	
xjc(1M)	
Application Server 9.1 Section 5ASC: Application Server Concepts	5
application(5ASC)	
cluster(5ASC)	
configuration(5ASC)	
domain(5ASC)	
dotted-names(5ASC)	
instance(5ASC)	773
loadbalancer(5ASC)	
logging(5ASC)	
monitoring(5ASC)	776
node-agent(5ASC)	
passwords(5ASC)	778
resource(5ASC)	779
security(5ASC)	
•	
Index	

Preface

> T A > 4 E

Both novice users and those familiar with Sun Java System Application Server can use online man pages to obtain information about the product 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 administration commands.
- Section 1M describes Application Server utility commands.
- Section 5ASC describes concepts that are related to Application Server administration.

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	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.	
	1	Separator. Only one of the arguments separated by this character can be specified at a time.	
DESCRIPTION	This section	on defines the functionality and behavior of the	

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

Application Server 9.1 Section 1: Administration Commands

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

Synopsis add-resources

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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 must be specified as

> http://www.sun.com/software/appserver/dtds/sun-resources 1 2.dtdinthe resources.xml file.

This command is supported in remote mode only.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target for which you are creating the resources. Valid values are

- server, which creates the resources for the default server instance server and is the default value
- domain, which creates the resources for the domain
- cluster_name, which creates the resources for every server instance in the cluster

--help

--target

Operands *xml_file_path*

• *instance_name*, which creates the resources for a particular server instance

The path to the XML file containing the resource(s) to be created. The XML file must reside in the <install-dir>/domains/domain1/config directory. If you specify a relative path or simply provide the name of the XML file, this command will prepend <install-dir>/domains/domain1/config to this operand.

An example XML file follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE resources PUBLIC
   "-//Sun Microsystems Inc.//DTD Application Server 9.1 Domain//EN"
   "*http://www.sun.com/software/appserver/dtds/sun-resources 1 2.dtd*">
<resources>
 <jdbc-connection-pool name="SPECjPool" steady-pool-size="100"</pre>
   max-pool-size="150" max-wait-time-in-millis="60000"
   pool-resize-quantity="2" idle-timeout-in-seconds="300"
   is-isolation-level-quaranteed="true"
   is-connection-validation-required="false"
   connection-validation-method="auto-commit"
   fail-all-connections="false"
   datasource-classname="oracle.jdbc.pool.OracleDataSource">
  roperty name="URL"
    value="jdbc:oracle:thin:@iasperfsol12:1521:specdb"/>
  cproperty name="User" value="spec"/>
  roperty name="Password" value="spec"/>
  property name="MaxStatements" value="200"/>
  cproperty name="ImplicitCachingEnabled" value="true"/>
 </idbc-connection-pool>
 <idbc-resource enabled="true" pool-name="SPECiPool"</pre>
   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:

16

EXAMPLE 1 Using the add-resources command (Continued)

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 apply-http-lb-changes – applies load balancer configuration changes to the load balancer

Synopsis apply-http-lb-changes

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
lb-name
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> Use the apply-http-lb-changes command to apply the changes in the load balancer configuration to the physical load balancer. The load balancer must already exist. To create a physical load balancer, use the create-http-lb 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 is 4848.

-s --secure

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

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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

Operands lb-name

The name of the load balancer to which changes are applied. The load balancer must already exist. You can create it with the create-http-lb command.

Examples EXAMPLE 1 Using the apply-http-lb-changes command

asadmin> apply-http-lb-changes --user admin --passwordfile file mylb Command apply-http-lb-changes executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also create-http-lb(1), create-http-lb-config(1)

Name backup-domain – performs a backup on the domain

Synopsis backup-domain [--domaindir *domain_directory*]

[--description description] [--echo={true | false}][--terse={true | 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.

-e --echo Setting to true will echo the command line statement on the

standard output. Default is false.

-t -- terse Indicates that any output data must be very concise, typically

avoiding human-friendly sentences and favoring

well-formatted data for consumption by a script. 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. If you have more than one domain, it is

mandatory to specify a domain name.

Examples EXAMPLE 1 Using backup-domain

asadmin> backup-domain --domaindir /opt/SUNWappserver/mydomaindir domain1

Successfully backed up the domain

Description: 1137030607263

Backup Filename: /opt/SUNWappserver/mydomaindir/domain1/backups/sjsas backup v00001.zip

Date and time backup was performed: Wed Jan 11 17:50:07 PST 2006

Domains Directory: /opt/SUNWappserver/mydomaindir

Domain Directory: /opt/SUNWappserver/mydomaindir/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 change-admin-password – changes the administrator password

Synopsis change-admin-password --user admin user

```
[--terse={true|false}] [ --echo ={true|false}]
[ --host hostname] [--port port-no]
```

[--secure | -s]

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 and for the new admin password (with confirmation).

Options -u -- user

The authorized domain administration server administrative username.

-t --terse

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption 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 is localhost.

-p --port

The port number of the domain administration server listening for administration requests. The default is port 4848.

-s --secure

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

```
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 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.

--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.

Examples EXAMPLE 1 Using the change-master-password command

This example assumes that you have used the asadmin login command before using 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 clear-ha-store – deletes tables in HADB

Synopsis clear-ha-store

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --haagentport port_number]
[--haadminpassword password] [--haadminpasswordfile filename]
[--hosts hadb_host_list] [--storeuser username]
[--storepassword password] [--dbsystempassword dbpassword]
database_name
```

Description Note – This command requires the HADB software. This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> This command deletes tables in HADB. Before you run this command, ensure that an HADB database instance exists. An HADB database instance can be created by using any of the following commands:

- create-cluster
- configure-ha-cluster
- create-ha-store

When specifying the hostlist interfaces explicitly for hosts with multiple network interfaces, use fully qualified hostnames.

The clear-ha-store command was named delete-session-store in the Sun Java System Application Server 7.1. The delete-session-store command is not included in this release of Sun Java System Application 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

-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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--haagentport

The name of the HA agent port. If not specified, the default port number is 1862.

--haadminpassword

The actual HADBM administation password. Using this option with the hadbm createdomain or hadbm create command requires that the password is entered each time any hadbm command is used.

The haadminpassword is different from the hadbm dbpassword command. You must use both passwords when using the following commands:

- hadbm create
- hadbm addnodes
- hadbm refragment
- --haadminpasswordfile

The file containing the HADBM administration password, storepassword, and dbsystempassword. These passwords must be defined in the following form:

```
HADBM_ADMINPASSWORD=password
HADBM_DBPASSWORD=storepassword
HADBM_SYSTEMPASSWORD=dbsystempassword
```

Where *password* is the actual administrator password.

--hosts

A comma-separated list of all the hosts that are part of the Management Agent.

--storeuser

This option specifies the username associated with the administrative instance.

--storepassword

The domain application server password associated with the administrative instance.

--dbsystempassword

The database password associated with the administrative instance.

Operands database_name The name of the HA database.

```
Examples EXAMPLE 1 Using clear-ha-store
```

```
asadmin> clear-ha-store --user admin --passwordfile password.txt
hadatabase1
```

Command clear-ha-store executed successfully

Exit Status 0 command executed successfully

1 error in executing the command

See Also configure-ha-cluster(1), create-cluster(1), create-ha-store(1)

Name configure-ha-cluster – configures an existing cluster to be highly available

Synopsis configure-ha-cluster

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --devicesize devicesize] [--haagentport port number]
[--haadminpassword password]
[--haadminpasswordfile file_name]
--hosts hadb-host-list [--autohadb={true|false}]
[ --portbase port_number]
[--property (name=value)[:name-value]*]
{clusterName}
```

Description Note – This command requires the HADB software. This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

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

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

This command is supported in remote mode only.

Options -t -- terse

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.

-e --echo

Setting to true will echo the 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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--devicesize

This is the device size in MegaBytes (MB). The valid range is between 208MB and 8+ gigabytes (GB).

--haagentport

This is the number of the HA agent port. The default is 1862.

--haadminpassword

This is the HA administrator's password.

--haadminpasswordfile

The file containing the high-availability password associated with the administrative instance. The password is defined in the following form:

HADBM_ADMINPASSWORD=*password*, HADBM_DBPASSWORD=*password*, HADBM_SYSTEMPASSWORD=*password*. Where *password* is the actual HA administrator password for the domain.

--hosts

This is a list of comma separated host names where the HADB instance is configured. The number of hosts must be greater than 1 and must be an even number. The same host names can be repeated. Use fully qualified hostnames when specifying the hostlist interfaces explicitly for hosts with multiple network interfaces.

--autohadb

If set to true, the HADB database associated with the cluster is automatically started, stopped, or deleted if you start, stop, or delete the cluster. The default is false. To override this setting, use the hadboverride option in start-cluster, stop-cluster, or delete-cluster.

--portbase

The starting port number for the HADB server. Default is 15000. Valid values are between 10000 and 63000.

--property

This is a list of property name/value pairs, which are separated by a colon.

The readable configuration attributes are as follows:

Variable	Range	Default
ConnectionTrace	true/false	false
CoreFile	true/false	false
DatabaseName		hadb
DataBufferPoolSize	16–2047	200 MB
DataDeviceSize	32–262144	1024 MB
DevicePath	n/a	n/a
EagerSessionThreshold	0-100	50 (% of NumberOfSessions)

Variable	Range	Default
Eager SessionTimeout	0-2147483647	120 seconds
EventBufferSize	0-2097152	0 MB
HistoryPath	n/a	n/a
InternalLogBufferSize	4–128	12 MB
JdbcUrl	n/a	n/a
LogBufferSize	4–2047	48 MB
MaxTables	100-1100	1100
NumberOfDataDevices	1-8	1
NumberOfLocks	20000-1073741824	50000
NumberOfSessions	1-10000	100
PackageName	n/a	V4.x.x.x
PortBase	10000-63000	15000
RelalgDeviceSize	32-262144	128 MB
SQLTraceMode	none/short/full	none
SessionTimeout	0-2147483647	1800 seconds
StartRepairDelay	0-100000	20 seconds
StatInterval	0-600	600 seconds
SyslogFacility	<facility></facility>	local0
SyslogLevel	<level></level>	warning
SyslogPrefix	<string></string>	hadb- <db_name></db_name>
TakeoverTime	500-16000	10000 MS

Operands clusterName

This is the name of the cluster that will be changed to high availability.

Examples EXAMPLE 1 Using the configure-ha-cluster command

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

asadmin> configure-ha-cluster --user admin --passwordfile passwordfile
--hosts red.iplanet.com.host1,red.iplanet.com.host2 cluster1
Command configure-ha-cluster executed successfully

Exit Status 0

command executed successfully

error in executing the command

See Also remove-ha-cluster(1)

1

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

Synopsis configure-ha-persistence

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --type persistencetype] [--frequency frequency]
[--scope scope] [--store jdbc_resource_jndi_name]
[--property (name=value)[:name=value]*]
clustername
```

Description Note – This command requires the HADB software. This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

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

The configure-ha-persistence command is available only with the enterprise profile.

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

-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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--tvpe

Set the persistence type to specify where session data is stored. The persistence types available are:

memory

If session persistence for the application server instance is disabled, this is the default persistence type. The memory persistence type provides no session persistence in a clustered environment. The memory persistence type is intended for development environments and should not be used for production.

file

This type provides no session persistence in a clustered environment. Use file persistence type to store session data in a file. If the instance becomes unavailable and

restarts, it can recover the session information that was last written to the file. The file persistence type is meant for development environments and should not be used for production.

ha

If session persistence for the application server instance is enabled, this is the default persistence type. This type allows you to store session data in the HADB. The ha persistence type enables failover of session information between application server instances in a cluster. The session information for each application server instance in a cluster is stored in the HADB. The session information is available to all other instances in the cluster. If an instance in a cluster becomes unavailable, another instance in the cluster can continue to serve the sessions that the now unavailable instance was serving.

--frequency

Set the persistence frequency to define the frequency at which the session state is stored in the HADB. The persistence frequencies available are:

web-method

The session is stored after every web request just before a response is sent back to the client. Use this frequency when you need very high availability of updated session states. This is the default.

time-based

The session is stored at the time interval defined in the reapIntervalSeconds property. A better throughput is achieved because the session is stored after a configurable time interval instead of after every web request.

--scope

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

modified-session

The entire session is stored only if it has been modified since the last time it was stored.

session

The entire session is stored every time session information is saved to the HADB. This is the default.

modified-attribute

Only the modified attributes of the session are stored. Using this mode can improve the throughput and response time significantly for applications in which only a small portion of the session state is modified for any given request.

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

• Call setAttribute() every time you modify the session state.

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

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

--property

Specify other session persistence properties.

Operands clustername

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

Examples EXAMPLE 1 Using configure-ha-persistence

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

Exit Status 0

command executed successfully

1 error in executing the command

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

Name configure-lb-weight – sets load balancing weights for clustered instances

Synopsis configure-lb-weight

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
 --cluster cluster name
instance-name=weight[:instance-name=weight]
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide

> The configure-lb-weight command assigns weight to the server instances in a cluster. Weights can be used for HTTP, RMI/IIOP and JMS load balancing. For the HTTP load balancer, the weights are used only if the load balancer's policy is set to weighted-round-robin. The load balancer policy is set in the create-http-lb-ref command or set command.

Use the weight to vary the load going to different instances in the cluster. For example, if an instance is on a machine with more capacity, give it a higher weight so that more requests are sent to that instance by the load balancer. The default weight is 100. If all instances have the default weight, the load balancer performs simple round robin load balancing.

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.

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 is 4848.

-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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--heln

Displays the help text for the command.

--cluster

The name of the cluster.

Operands *instance-name=weight*

The name of the instance and the weight you are assigning it. The weight must be an integer. The pairs of instances and weights are separated by colons. For example instance1=1:instance2=4 means that for every five requests, one goes to instance1 and four go to instance2. A weight of 1 is the default.

Examples EXAMPLE 1 Using the configure-lb-weight command

The following command assigns weights of 1, 1, and 2 to instances i1, i2, and i3 in the cluster1 cluster.

```
asadmin> configure-lb-weight --user admin --passwordfile passwords.txt --cluster cluster1 i1=1:i2=1:i3=2

Command configure-lb-weight executed successfully.
```

Exit Status 0 command executed successfully

1 error in executing the command

See Also create-http-lb-ref(1)create-cluster(1)

Name configure-webservice-management – sets the monitoring or maxhistorysize attributes of a deployed web service Synopsis configure-webservice-management [--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [--monitoring = {OFF | LOW | HIGH}] [--maxhistory maxhistory-size] webservice-end-point **Description** Use this command to configure the monitoring or the maxhistory attributes of a deployed webservice. 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 is 4848. If set to true, uses SSL/TLS to communicate with -s --secure the domain administration server. The authorized domain administration server -u --user 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, including the full path, 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.

--monitoring

--maxhistorysize

Operands webservice-end-point

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help Displays the help text for the command.

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: 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.

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

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

asadmin> 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

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

Where <code>jaxrpc-simple#jaxrpc-simple.war#HelloIF</code> is the fully qualified name of a webservice endpoint.

Exit Status 0 command executed successfully

1 error in executing the command

42

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

Synopsis copy-config

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

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

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

Options -t--terse

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.

-e --echo

Setting to true will echo the command line statement on the standard output. Default is false.

-I --interactive

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

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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--systemproperties

Optional attribute name/value pairs for configuring the resource. The following properties are available:

HTTP LISTENER PORT

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

HTTP SSL LISTENER PORT

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

IIOP LISTENER PORT

This property specifies which ORB listener port for IIOP connections orb-listener-1 listens on.

IIOP SSL LISTENER PORT

This property specifies which ORB listener port for IIOP connections the IIOP listener called SSI 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 source_configuration_name

The name of the configuration you are copying.

destination_configuration_name

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

Examples EXAMPLE 1 Using the copy-config command

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

Command copy-config executed successfully.

Exit Status 0

command executed successfully

1

error in executing the command

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

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

Synopsis create-admin-object --restype *aorestype*

--raname resource_adapter_name

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host]

[--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

[--enabled ={true | false}] [--target target] [--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.

The machine name where the domain administration server -H --host

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 is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

administration server.

The authorized domain administration server -u --user

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.

The --passwordfile option specifies the name, including --passwordfile

> the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target on which you are creating the administered object. 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

Specifies if this object is enabled. The default value is true.

--help

--target

--enabled

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

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

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

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

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

This command is supported in remote mode only.

Options -t--terse

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.

-e --echo

Setting to true will echo the 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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--target

Specifies the target for which you are creating the application reference. Valid values are

- server, which creates the application reference for the default server instance server and is the default value
- cluster_name, which creates the application reference for every server instance in the cluster
- instance_name, which creates the application reference for the named unclustered server instance

--enabled

Indicates whether the application should be enabled (that is, loaded). This value will take effect only if the application is enabled at the global level. The default is true.

--virtualservers

Comma-separated list of virtual server IDs on which to deploy. This option applies only to Web modules (either standalone or in a Java EE application). If this option is not specified, the application is deployed to all virtual servers except the administrative server, asadmin.

Operands reference name

The name of the application or module, which can be a Java EE application, Web module, EJB module, connector module, application client module, or lifecycle module.

Examples EXAMPLE 1 Using the create-application-ref command

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

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

Exit Status 0 command executed successfully

1 error in executing the command

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

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

Synopsis create-audit-module --classname classname [--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help]

[--property (name=value)[:name=value]*] [--target target_name] 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 --classname Java class which implements this audit module.

> -t --terse Indicates that any output data must be very concise, typically

> > avoiding human-friendly sentences and favoring

well-formatted data for consumption by a script. Default is

false.

-e --echo Setting to true will echo the 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.

The HTTP/S port for administration. This is the port to -p --port

which you should point your browser in order to manage the

domain. For example, http://localhost:4848.

The default port number is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

administration server.

The authorized domain administration server -u --user

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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

optional attributes name/value pairs of provider implementation specific attributes.

Specifies the target on which you are creating the audit module. Valid values are

- server, which creates the audit module for the default server instance server and is the default value
- configuration_name, which creates the audit module for the named configuration

--help

--property

--target

- 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

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 --classname realm_class [--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [--property (name=value)[:name=value]*]

[--target target_name] auth_realm_name

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

escription	Adds the named authentication realm. This command is supported in remote mode only.	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
		m1 1 1.

uppercase letters.

The --passwordfile option specifies the name, including the full path, 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

--passwordfile

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target on which you are creating the realm. Valid values are

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

Java class which implements this realm.

--help

--target

--classname

--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

Where db is the auth realm created.

Exit Status 0 command executed successfully

1 error in executing the command

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

Name create-cluster – creates a cluster

Synopsis create-cluster

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --config config name]
[--systemproperties (name=value)[:name=value]*]
[--hosts hadb-host-list]
[--haagentport port number]
[--haadminpassword password]
[--haadminpasswordfile file_name] [--devicesize devicesize]
[--haproperty (name=value)[:name=value]*]
[--autohadb=false] [--portbase port_number]
cluster name
```

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

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

If you do not use the --config option, the command creates a standalone cluster with a configuration named *cluster name*-config.

If the HADB software is installed, you can create the HADB database associated with the cluster. To create it, specify the HADB hosts option. In addition, optionally specify any other HADB options such as haagentport and devicesize. The created database has the same name as the cluster, and includes all the correct tables.

The cluster must be a standalone cluster in order to successfully associate an HADB database with it. standalone cluster does not share its configuration with another cluster or another standalone instance. A standalone cluster does not share its configuration with another cluster or another standalone instance.

If you prefer to associate the HADB database to the cluster later, use configure-ha-cluster.

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

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

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

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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--config

Creates a shared cluster. The specified configuration name must exist and must not be default-config (the standalone cluster configuration template) or a standalone configuration (including server-config). If this option is omitted, a standalone cluster is created.

--systemproperties

Defines system properties for the configuration created for by the cluster. These properties override the property values in the default-config configuration. The following properties are available:

HTTP LISTENER PORT

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

HTTP SSL LISTENER PORT

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

IIOP LISTENER PORT

This property specifies which ORB listener port for IIOP connections orb-listener-1 listens on.

IIOP SSL LISTENER PORT

This property specifies which ORB listener port for IIOP connections the IIOP listener called SSL listens on.

IIOP SSL MUTUALAUTH PORT

This property specifies which ORB listener port for IIOP connections the IIOP listener called SSL MUTUALAUTH listens on.

JMX SYSTEM CONNECTOR PORT

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

--hosts

This option is valid only if the HADB software is installed. A list of comma-separated host names where the HADB instance is configured. The number of hosts must be greater than 1 and must be an even number. The same host names can be repeated. Use fully-qualified hostnames when specifying the hostlist interfaces explicitly for hosts with multiple network interfaces.

--haagentport

This option is valid only if the HADB software is installed. The number of the HA agent port. The default is 1862.

--haadminpassword

This option is valid only if the HADB software is installed. The HA administrator's password. If not specified, the Domain Administration Server password is used.

--haadminpasswordfile

This option is valid only if the HADB software is installed. The file containing the high-availability password associated with the administrative instance. The password is defined in the following form:

```
HADBM_ADMINPASSWORD=password
HADBM_DBPASSWORD=password
HADBM_SYSTEMPASSWORD=password
```

Where *password* is the actual HA administrator password for the domain. If the HA administrator password is not specified, the Domain Administration Server password is used.

--devicesize

This option is valid only if the HADB software is installed. Configure the device size for use with HADB. The value is in megabytes (Mbytes). The valid range is between 64 Mbytes and 8,000+ gigabytes (GBytes).

--haproperty

This option is valid only if the HADB software is installed. The high-availability property name/value pairs separated by a colon.

--autohadb

This option is valid only if the HADB software is installed. If set to true, the HADB database associated with the cluster is automatically started, stopped, or deleted if you start, stop, or

delete the cluster. The default is false. To override this setting, use the hadboverride option in start-cluster, stop-cluster, or delete-cluster.

--portbase

This option is valid only if the HADB software is installed. The starting port number for the HADB server. Default is 15200. Valid values are between 10000 and 63000.

Operands *cluster name*

A unique identifier for the cluster to be created.

Examples EXAMPLE 1 Using the create-cluster command

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

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

EXAMPLE 2 Creating HADB when creating cluster

This example requires the HADB software and a domain that is created with theenterprise profile.

The following command creates an HADB database on hosts host1 and host2 while creating the cluster cluster1:

```
asadmin> create-cluster --user admin1
--passwordfile passwords.txt --hosts hos1,host2 cluster1
Command create-cluster executed successfully.
```

Exit Status 0

command executed successfully

1 error in executing the command

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

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

Synopsis create-connector-connection-pool

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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]*]

Description The create-connector-connection-pool adds a new connector connection pool with the specified connection pool name.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	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.

connector_connection_pool_name

--passwordfile

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The target option is deprecated.

The name of the resource adapter.

The name of the connection definition.

The minimum and initial number of connections maintained in the pool. The default value is 8.

--help

--target

--raname

--connectiondefinition

--steadypoolsize

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	Quantity by which the pool will scale-up or scale-down the number of connections. Scale-up: When the pool has no free connections, pool will scale-up by this quantity. Scale-down: All the invalid and idle connections are removed, sometimes resulting in removing connections of quantity greater than this value. Steadypoolsize will be ensured. Possible values are from 0 to MAX_INTEGER. The default value is 2.
idletimeout	The maximum time that a connection can remain idle in the pool. After this amount of time, the pool can close this connection. The default value is 300.
failconnection	If set to true, all connections in the pool are closed if a single validation check fails. This parameter is mandatory if the is-connection-validation-required is set to true. Legal values are on, off, yes, no, 1,0, true or false. The default value is false.
transactionsupport	Indicates the level of transaction support that this pool will have. Possible values are XATransaction, LocalTransaction and NoTransaction. This attribute can have a value lower than or equal to but not higher than the resource adapter's transaction support attribute. The resource adapter's transaction support attribute has an order of values, where XATransaction is the highest, and NoTransaction the lowest.
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.
- ' ' 1	TTI C.1 (* 1.1 (.1

 ${\bf Operands} \quad {\it connector_connection_pool_name}$

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
- $--connection definition \ javax.jms. Queue Connection Factory \ jms/q Conn Pool$

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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile *filename*] [--help]

[--target *target*]

--poolname connectorConnectionPoolName [--enabled=true]

[--description text] indi_name

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

Options	-tterse	Indicates that any output data must be very concise, typically

avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is

false.

-e --echo Setting to true will echo the 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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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.

--help

--target

--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 *indi_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 a domain whose profile is the developer profile.

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 a domain whose profile is the cluster profile.

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={true|false}][ --echo={true|false} ]
          [ --interactive={true|false} ] [ --host host]
          [--port port] [--secure| -s ] [ --user admin_user]
          [--passwordfile filename] [--help]
            --poolname connector connection pool name
          [--principals principal_name1[, principal_name2]* |
          --usergroups user_group1[, user_group2*]
           --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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.

-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.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--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 --mappe

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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]
[--passwordfile filename] [--help]
 --restype type
 --factoryclassname classname [--enabled=true]
[--description text] [--property (name=value)[:name=value]*]
indi 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 -tterse	Indicates that any output data must be very concise, typically
	indicated that any carp at data made of very contense, typically

avoiding human-friendly sentences and favoring

well-formatted data for consumption by a script. Default is

false.

-e --echo Setting to true will echo the 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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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.

--help

--target

		 instance_name, which deploys the component to a particular sever instance.
	resourcetype	Theresource type option is deprecated. Userestype 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-resourceuser adminpasswordfile passwords.txtrestype topicfactoryclass 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 [--user user] [--passwordfile passwordfile]

[(--adminport port_number | --portbase portbase)]

[(--profile developer | cluster | enterprise ] --template domain_template)]

[--domaindir domain_directory/domains]

[--instanceport port_number] [--savemasterpassword=false]

[--domainproperties (name=value)[:name=value]*

]

[--savelogin=false] [--terse=false]

[--echo=false] [--interactive=true]

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 default directory for domains. 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.

You choose an appropriate profile for the domain, depending on the applications that youwant to run on your new domain. You can choose the developer, cluster, or enterprise profile for the domain you create.

This command is supported in local mode only.

Options	user	The username of the adminstrator of the domain.	
	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	
	-eecho	Setting to true will echo the 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. --profile The profile of the domain. A usage profile depicts how a particular domain is going to be used. It determines how the templates for various files are customized. Currently, only

> Valid values for this option are: developer, cluster, and enterprise

the customization for domain.xml template is supported.

Note – Profile names are case-sensitive. Use all profile names in lower case only.

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.

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. This option is mandatory unless you specify a value for the --portbase option.

The file containing the domain application server password associated with the administrative instance. The create-domain command reads values for AS_ADMIN_PASSWORD and the AS ADMIN MASTERPASSWORD from this file. The password is defined in the following form:

AS_ADMIN_PASSWORD=password, where password is the actual administrator password for the domain. 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_PASSWORD or AS_ADMIN_MASTERPASSWORD are not in the passwordfile, create-domain command prompts for admin password and master password.

--template

--adminport

--passwordfile

-t --terse

Indicates that any 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.

--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.

--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:

- 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 the ORB listener port for IIOP connections on which orb-listener-1 listens.
- http.ssl.port: Specifies the port number for http-listener-2. Valid values are 1 to 65535. On UNIX, to create sockets that listen on ports 1–1024, you need superuser privileges.
- orb.ssl.port: Specifies the ORB listener port for IIOP connections on which the IIOP listener called SSL listens.
- orb.mutualauth.port: Specifies the ORB listener port for IIOP connections on which the IIOP listener called SSL MUTUALAUTH listens.

Determines the number with which the port assignment should start. A domain uses a certain number of ports that are statically assigned. The portbase value determines where the assignment should start. Choose this value judiciously. The values for the ports are calculated as follows: Admin port: portbase + 48, HTTP listener port: portbase + 80, IIOP listener port: portbase + 86. See the output of this command for a complete list of occupied ports, when --portbase option is specified.

Note – The --portbase option cannot be used with the --adminport or the --instanceport option.

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

--portbase

--savelogin

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 (developer profile)

The following command creates domain4 domain with developer profile.

```
asadmin>create-domain --adminport 4848 --profile developer domain4
Please enter the admin user name>admin
Please enter the admin password>
Please enter the admin password again>
Please enter the master password>
Please enter the master password again>
Using port 4848 for Admin.
Using default port 8080 for HTTP Instance.
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 being created with profile:developer, as specified on command line or environment.
Security Store used should be JKS
Domain domain4 created.
```

EXAMPLE 2 Using the create-domain command (enterprise profile)

The following command creates sampleDomain domain with enterprise profile in the /export/domains directory.

```
asadmin> create-domain --domaindir /export/domains
--profile enterprise --adminport 7070 --adminuser admin
--instanceport 7071 sampleDomain
Please enter the admin password>
Please enter the admin password again>
Please enter the master password>
Please enter the master password again>
Using port 7070 for Admin.
Using default port 7071 for HTTP Instance.
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 being created with profile:enterprise, as specified
```

EXAMPLE 2 Using the create-domain command (enterprise profile) (Continued)

by variable AS_ADMIN_PROFILE in configuration file. Security Store used should be NSS Domain sampleDomain created.

EXAMPLE 3 Using the create-domain command (savelogin)

The following command creates the myDomain domain with the enterprise profile and saves the admin username and password.

```
asadmin> create-domain --adminport 8282 --adminuser admin
--savelogin=true mvDomain
Please enter the admin user name>admin
Please enter the admin password>
Please enter the admin password again>
Please enter the master password>
Please enter the master password again>
Using port 8282 for Admin.
Using default port 8080 for HTTP Instance.
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 being created with profile:enterprise, as specified by variable
AS ADMIN PROFILE in configuration file.
adSecurity Store used should be NSS
Domain myDomain created.
Login information relevant to admin user name [admin] for this domain [myDomain]
 stored at [/.asadminpass] successfully.
Make sure that this file remains protected. Information stored in this file will be
used by asadmin commands to manage this domain.
```

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser

option on subsequent operations to this particular domain.

--passwordfile

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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 valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

--help

--target

--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

Command create-file-user executed successfully

Where, the sample_user is the file user created.

Exit Status 0 command executed successfully

1 error in executing the command

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

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

Synopsis create-ha-store

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

Description Note – This command requires the HADB software. This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

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

This command is supported in remote mode only.

Options -t--terse

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.

-e --echo

Setting to true will echo the command line statement on the standard output. Default is

-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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--haagentport

The name of the HA agent port. If not specified, the default port number is 1862.

--haadminpassword

The actual HADBM administation password. Using this option with the hadbm createdomain or hadbm create command requires that the password is entered each time any hadbm command is used.

The haadminpassword is different from the hadbm dbpassword command. You must use both passwords when using the following commands: hadbm create, hadbm addnodes, hadbm refragment.

--haadminpasswordfile

The file containing the HADBM administration password, storepassword, and dbsystempassword. These passwords must be defined in the following form: HADBM_ADMINPASSWORD=password, HADBM_DBPASSWORD=storepassword, HADBM_SYSTEMPASSWORD=dbsystempassword. Where password is the actual administrator password.

--hosts

A comma-separated list of all the hosts that are part of the Management Agent.

--storeuser

This option specifies the username associated with the administrative instance.

--storepassword

The domain application server password associated with the administrative instance.

--dbsystempassword

The database password associated with the administrative instance.

Operands database_name

The name of the HA database.

Examples EXAMPLE 1 Using create-ha-store

The create-ha-store command executed successfully

Exit Status 0

command executed successfully

1

error in executing the command

See Also clear-ha-store(1), configure-ha-cluster(1)

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

Synopsis create-http-health-checker

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
 [ --url "/"]
 [--interval 30] [--timeout 10]
 [--config config_name] target
```

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> This command creates a health checker for a specified load balancer configuration. A health checker is unique for the combination of target and load balancer configuration.

> This command only works with the native load balancer provided with the Sun Java System Application Server. It does not work with other load balancers.

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.

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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--url

The URL to ping to determine whether the instance is healthy.

--interval

The interval in seconds the health checker waits between checks of an unhealthy instance to see whether it has become healthy. The default value is 30 seconds. A value of 0 disables the health checker.

--timeout

The interval in seconds the health checker waits to receive a response from an instance. If the health checker has not received a response in this interval, the instance is considered unhealthy.

--config

The load balancer configuration for which you create the health-checker. If you do not specify a configuration, the command creates a health checker for every load balancer configuration associated with the target. If no configuration references the target, the command fails.

Operands target

Specifies the target to which the health checker applies.

Valid values are:

- cluster_name, which specifies the health checker will monitor all instances in the cluster.
- stand-alone_instance_name, which specifies that the health checker will monitor this stand-alone instance.

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

asadmin> create-http-health-checker --user admin

--passwordfile password.txt --config mycluster-http-lb-config mycluster

Command create-http-health-checker executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

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

Name create-http-lb - creates a load balancer

Synopsis create-http-lb

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile *filename*] [--help] --devicehost device_host_or_IP_address --deviceport device_port

[--autoapplyenabled=false] [--sslproxyhost proxy_host]

[--sslproxyport proxy_port] [--target target] [--lbpolicy lbpolicy] [--lbpolicymodule lb_policy_module]

[--healthcheckerinterval 10] [--healthcheckertimeout 10]

[--lbenableallinstances=true] [--lbenableallapplications=true] [--lbweight instance=weight[:instance

[--property (name=value)[:name=value]*

1 load balancer name

Description

Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

Use the create-http-lb command to create a load balancer, including the load balancer configuration, target reference, and health checker. A load balancer is a representation of the actual load balancer device, defined by its device host and port information. Once you've created the load balancer, you can automatically apply changes made to the load balancer configuration without running export-http-lb-config and manually copying the generated load balancer configuration file to the web server instance. Set autoapplyenabled to true to automatically apply changes.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	The HTTP/S port for administration. This is the port to

The default port number is 4848.

which you should point your browser in order to manage the

domain. For example, http://localhost:4848.

-s --secure

-u --user

--passwordfile

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

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command. --help --devicehost The device host or the IP address of the load balancing device. This host or IP is where the physical load balancer will reside. --deviceport The port used to communicate with the load balancing device. It must be SSL enabled. If set to true, changes to the load balancer configuration are --autoapplyenabled automatically pushed to the physical load balancer. If set to false, the changes won't be automatically applied. Use the command apply-http-lb-changes to apply the changes manually. The default is false. --sslproxyhost The proxy host used for outbound HTTP. --sslproxyport The proxy port used for outbound HTTP. Specifies the target to which the load balancer applies. --target Valid values are: cluster_name, which specifies that requests for this cluster will be handled by the load balancer. stand-alone_instance_name, which specifies that requests for this stand-alone instance will be handled by the load balancer. --lbpolicy The policy the load balancer follows to distribute load to the server instances in a cluster. Valid values are round-robin, weighted-round-robin, and user-defined. If you choose user-defined, specify a load balancer policy module with the lbpolicymodule option. If you choose weighted-round-robin, assign weights to the server instances using the configure-lb-weight command. The default is round-robin. --lbpolicymodule If your target is a cluster and the load balancer policy is user-defined, use this option to specify the full path and name of the shared library of your load balancing policy module. The shared library needs to be in a location accessible by the web server. --healthcheckerurl The URL to ping to determine whether the instance is healthy.

healthcheckerinterval	The interval in seconds the health checker waits between checks of an unhealthy instance to see whether it has become healthy. The default value is 10 seconds. A value of 0 disables the health checker.
healthcheckertimeout	The interval in seconds the health checker waits to receive a response from an instance. If the health checker has not received a response in this interval, the instance is considered unhealthy. The default value is 10 seconds.
lbenableallinstances	Enables all instances in the target cluster for load balancing. If the target is a server instance, enables that instance for load balancing.
lbenableallapplications	Enables all applications deployed to the target cluster or instance for load balancing.
lbweight	The name of the instance and the weight you are assigning it. The weight must be an integer. The pairs of instances and weights are separated by colons. For example instance1=1:instance2=4 means that for every five requests, one goes to instance1 and four go to instance2. A weight of 1 is the default.
responsetimeout	The time in seconds within which a server instance must return a response. If no response is received within the time period, the server is considered unhealthy. If set to a positive number, and the request is idempotent, the request is retried. If the request is not idempotent, an error page is returned. If set to 0 no timeout is used. The default is 60.
httpsrouting	If set to true, HTTPS requests to the load balancer result in HTTPS requests to the server instance. If set to false, HTTPS requests to the load balancer result in HTTP requests to the server instance. The default is false.
reloadinterval	The time, in seconds, that the load balancer takes to check for an updated configuration. When detected, the configuration file is reloaded. The default value is 60 seconds. A value of 0 disables reloading.
monitor	If set to true, monitoring of the load balancer is switched on. The default value is false.
routecookie	This option is deprecated. The value is always true.
property	Optional attribute name/value pairs for configuring the load balancer.

Operands \(lb_name \)

The name of the new load balancer. This name must not conflict with any other load balancers in the domain.

Examples \(\text{EXAMPLE 1} \) Using the create-http-lb command \(\text{asadmin} \) -reate-http-lb --user admin --passwordfile password.txt \(\text{--autoapplyenabled=true} \) --devicehost host1 --deviceport 5555 \(\text{mylb} \) Command create-http-lb executed successfully.

Exit Status \(0 \) command executed successfully \(1 \)

error in executing the command

See Also delete-http-lb(1), list-http-lbs(1), create-http-lb-config(1)

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

Synopsis create-http-lb-config

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --responsetimeout 60]
[ --httpsrouting=false] [--reloadinterval 60]
[ --monitor=false] [ --property (name=value)[:name=value]*]
  --target target | config_name
```

Description

Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in *Sun Java System Application Server 9.1 Administration Guide*.

Use the create-http-lb-config command to create a load balancer configuration. This configuration applies to load balancing in the HTTP path. After using this command to create the load balancer configuration file, create the load balancer by running create-http-lb.

You must specify either a target or a configuration name, or both. If you don't specify a target, the configuration is created without a target and you add one later using create-http-lb-ref If you don't specify a configuration name, a name is created based on the target name. If you specify both, the configuration is created with the specified name, referencing the specified target.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

--passwordfile

--help

--responsetimeout

The time in seconds within which a server instance must return a response. If no response is received within the time period, the server is considered unhealthy. If set to a positive number, and the request is idempotent, the request is retried. If the request is not idempotent, an error page is returned. If set to 0 no timeout is used. The default is 60.

--httpsrouting

If set to true, HTTPS requests to the load balancer result in HTTPS requests to the server instance. If set to false, HTTPS requests to the load balancer result in HTTP requests to the server instance. The default is false.

--reloadinterval

The interval between checks for changes to the load balancer configuration file loadbalancer.xml. When the check detects changes, the configuration file is reloaded. A value of 0 disables reloading.

--monitor

Specifies whether monitoring is enabled. The default is false.

--routecookie

This option is deprecated. The value is always true.

--property

Optional attribute name/value pairs for configuring the load balancer.

--target

Specifies the target to which the load balancer configuration applies. If you don't specify a target, the load balancer configuration is created without a target. You can specify targets later using the command create-http-lb-ref.

Valid values are:

- cluster_name, which specifies that requests for this cluster will be handled by the load balancer.
- stand-alone_instance_name, which specifies that requests for this stand-alone instance will be handled by the load balancer.

Operands *config_name*

The name of the new load balancer configuration. This name must not conflict with any other load balancer groups, agents, configurations, clusters, or sever instances in the domain. If you don't specify a name, the load balancer configuration name is based on the target name, target_name-http-lb-config.

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

asadmin> create-http-lb-config --user admin --passwordfile file --target mycluster

mylbconfigname

Command create-http-lb-config executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

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

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

Synopsis create-http-lb-ref

```
[--terse={true|false}][ --echo={true|false} ]
[--interactive={true|false}] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
--config config_name | --lbname load_balancer_name
[--lbpolicy round-robin] [--lbpolicymodule lb_policy_module]
[--healthcheckerurl url] [--healthcheckerinterval 10]
[--healthcheckertimeout 10] [--lbenableallinstances=true]
[--lbenableallapplications=true] [--lbweight instance=weight[:instance=weight]*]
target
```

Description

Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in *Sun Java System Application Server 9.1 Administration Guide.*

Use the create-http-lb-ref command to:

- Add an existing cluster or server instance to an existing load balancer configuration or load balancer. The load balancer forwards the requests to the clustered and stand-alone instances it references.
- Set the load balancing policy to round-robin, weighted round-robin, or to a user-defined policy.
- Configure a health checker for the load balancer. Any health checker settings defined here
 apply only to the target. If you do not create a health checker with this command, use
 create-http-health-checker.
- Enable all instances in the target cluster for load balancing, or use enable-http-lb-server to enable them individually.
- Enable all applications deployed to the target for load balancing, or use enable-http-lb-application to enable them individually.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	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. The HTTP/S port for administration. This is the -p --port port to which you should point your browser in order to manage the domain. For example, http://localhost:4848. The default port number is 4848. If set to true, uses SSL/TLS to communicate with -s --secure the domain administration server. The authorized domain administration server -u --user 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.

The --passwordfile option specifies the name, including the full path, 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

--passwordfile

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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies which load balancer configuration to which to add clusters and server instances. Specify either a load balancer configuration or a load balancer. Specifying both results in an error.

Specifies the load balancer to which to add clusters and server instances. Specify either a load balancer configuration or a load balancer. Specifying both results in an error.

The policy the load balancer follows. Valid values are round-robin, weighted-round-robin, and user-defined. If you choose user-defined, specify a load balancer policy module with the lbpolicymodule option. If you choose weighted-round-robin assign weights to the server instances using the configure-lb-weight command. The default is round-robin.

--help

--config

--lbname

--lbpolicy

lbpolicymodule	If your load balancer policy is user-defined, use

this option to specify the full path and name of the shared library of your load balancing policy module. The shared library needs to be in a location accessible by the web server.

iocation accessible by the web server.

--healthcheckerurl The URL to ping to determine whether the

instance is healthy.

--healthcheckerinterval The interval in seconds the health checker waits

between checks of an unhealthy instance to see whether it has become healthy. The default value is 30 seconds. A value of 0 disables the health

checker.

--healthcheckertimeout The interval in seconds the health checker waits

to receive a response from an instance. If the health checker has not received a response in this interval, the instance is considered

unhealthy. The default is 10.

--lbenableallinstances Enables all instances in the target cluster for load

balancing. If the target is a server instance, enables that instance for load balancing. The

default value is true.

--lbenableallapplications Enables all applications deployed to the target

cluster or instance for load balancing. The

default value is true.

--lbweight The name of the instance and the weight you are

assigning it. The weight must be an integer. The pairs of instances and weights are separated by colons. For example instance1=1:instance2=4 means that for every five requests, one goes to instance1 and four go to instance2. A weight of 1

is the default.

Operands target Specifies which cluster or instance to add to the load balancer. Valid values are:

- cluster_name, which specifies that requests for this cluster will be handled by the load balancer.
- stand-alone_instance_name, which specifies that requests for this stand-alone instance will be handled by the load balancer.

```
Examples EXAMPLE 1 Using the create-http-lb-ref command to add a cluster to a load balancer configuration
            asadmin> create-http-lb-ref --user admin --passwordfile file
            --config mylbconfig cluster2
            Command create-http-lb-ref executed successfully.
            EXAMPLE 2 Using the create-http-lb-ref command to add a cluster to a load balancer
            asadmin> create-http-lb-ref --user admin --passwordfile file
            -- lbname mylb cluster2
            Command create-http-lb-ref executed successfully.
            EXAMPLE 3 Using the create-http-lb-ref command to configure a health checker and load balancing
            policy, and enable instances and applications
            asadmin> create-http-lb-ref --user admin --passwordfile file
            --config mylbconfig --lbpolicy weighted-round-robin
            --healthcheckerinterval 40 --healthcheckertimeout 20
            --lbenableallinstances=true --lbenableallapplications=true cluster2
            Command create-http-lb-ref executed successfully.
            EXAMPLE 4 Using the create-http-lb-ref command to set a user-defined load balancing policy
            asadmin> create-http-lb-ref --user admin --passwordfile file
            --lbpolicy user-defined --lbpolicymodule /user/modules/module.so
            --config mylbconfig cluster2
            Command create-http-lb-ref executed successfully.
Exit Status 0
                                           command executed successfully
            1
                                           error in executing the command
```

See Also delete-http-lb-ref(1), create-http-health-checker(1), enable-http-lb-server(1), enable-http-lb-application(1), list-http-lb-configs(1), list-http-lbs(1) configure-lb-weight(1)

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

Synopsis create-http-listener

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
--listeneraddress address --listenerport listener_port
--defaultvs virtual_server [--servername server_name]
[--acceptorthreads acceptor-threads] [--xpowered={true|false}]
[ --redirectport redirect_port] [--securityenabled={true|false}]
[ --enabled ={true|false}] [ --target server] listener_id
```

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

> Note - If you edit the special HTTP listener named admin-listener, you must restart the server for the changes to take effect. The Administration Console does not tell you that a restart is required in this case.

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.

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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--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

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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.

--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 valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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 standalone 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
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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
 --listeneraddress address
[--iiopport iiop-port-number] [--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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--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 valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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 valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

```
asadmin> create-iiop-listener --user admin
--passwordfile passwords.txt --host host1 --port 4848
--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 --nodeagent name
         [--terse={true|false}][ --echo={true|false} ]
          [ --interactive={true|false} ] [ --host host]
          [--port port] [--secure| -s ] [ --user admin_user]
          [--passwordfile filename] [--help]
          [ --config config_name | --cluster cluster_name]
           [--systemproperties (name=value)[:name=value]*]
          instance_name
```

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> 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 -- 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.

-t --terse

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.

-e --echo

Setting to true will echo the 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 is 4848.

-s --secure

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

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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--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.

--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:

HTTP LISTENER PORT

This property specifies the port number of the port that is used to listen for HTTP requests. Valid values are 1–65535. On UNIX, creating sockets that listen on ports 1–1024 requires superuser privileges.

HTTP SSL LISTENER PORT

This property specifies the port number of the port that is used to listen for HTTPS requests. Valid values are 1–65535. On UNIX, creating sockets that listen on ports 1–1024 requires superuser privileges.

IIOP LISTENER PORT

This property specifies the port number of the port that is used for IIOP connections.

IIOP SSL LISTENER PORT

This property specifies the port number of the port that is used for secure IIOP connections.

IIOP SSL MUTUALAUTH PORT

This property specifies the port number of the port that is used for secure IIOP connections with client authentication.

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 *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 4848 --nodeagent agent1 instance1
Command create-instance executed successfully
```

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

EXAMPLE 2 Using the create-instance command with systemproperties

```
asadmin> create-instance --user admin --passwordfile password.txt
--host myhost --port 4848 --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
```

EXAMPLE 2 Using the create-instance command with systemproperties (Continued)

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

Errors 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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

--target

	 instance_name, which creates the resource for a particular server instance
mailhost	The DNS name of the default mail server. The connect methods of the Store and Transport objects use this value if a protocol-specific host property is not supplied. The name must be resolvable to an actual host name.
mailuser	The 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 *indi_name*

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

Examples EXAMPLE 1 Using the create-javamail-resource command

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

asadmin> create-javamail-resource --user admin
--passwordfile passwords.txt --host fuyako --port 7070
--mailhost localhost --mailuser sample
--fromaddress sample\\@sun\\.com mail/MyMailSession
Command create-javamail-resource executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

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

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

Synopsis create-jdbc-connection-pool [--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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)

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.

[:name=value]*] connectionpoolid

11	,
-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
-Iinteractive	If set to true (default), only the required password options are prompted.
-Hhost	The machine name where the domain administration server is running. The default value is localhost.
-pport	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 is 4848.
-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-eecho -Iinteractive -Hhost -pport

-u --user

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for

AS ADMIN MASTERPASSWORD is changeit.

Displays the help text for the command.

This option is deprecated.

The name of the vendor—supplied JDBC

datasource resource manager.

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.

The minimum and initial number of

connections maintained in the pool. The default

value is 8.

The maximum number of connections that can

be created. The default value is 32.

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.

Quantity by which the pool will scale-up or

scale-down the number of connections. Scale-up: When the pool has no free

connections, pool will scale-up by this quantity. Scale-down: All the invalid and idle connections are removed, sometimes resulting in removing connections of quantity greater than this value.

--help

--target

--datasourceclassname

--restype

--steadypoolsize

--maxpoolsize

--maxwait

--poolresize

Steadypoolsize will be ensured. Possible values are from 0 to MAX INTEGER. 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. Optional attribute name/value pairs for --property configuring the connection pool. **Operands** connection poolid 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

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

 $\textbf{See Also} \quad delete-jdbc\text{-}connection\text{-}pool (1), list\text{-}jdbc\text{-}connection\text{-}pools (1)$

Name create-jdbc-resource – creates a JDBC resource with the specified JNDI name

Synopsis create-jdbc-resource

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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.

--help

--target

• *instance_name*, which deploys the component to a particular sever instance. --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. Determines whether the JDBC resource is enabled at --enabled 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_

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-imsdest

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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.

Setting to true will echo the 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 is 4848.

-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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--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 valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

-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:

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.

To modify the value of this property or to specify other physical destination properties, use the <code>install_dir/imq/bin/imqcmd</code> command. See the <code>Sun Java System Message Queue 3.7 UR1 Administration Guide</code> 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-host – creates a JMS host

Synopsis create-jms-host

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

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

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

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser

option on subsequent operations to this particular domain.

--passwordfile

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target for which you are creating the JMS host. Valid targets are

- server, which creates the JMS host for the default server instance and is the default target.
- configuration_name, which creates the JMS host for the named configuration

--help

--target

•	cluster_name, which creates the JMS host for every server
	instance in the cluster

• *instance_name*, which creates the JMS host for a particular server instance

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

--mqhost The host name for the JMS service. The default value is

localhost.

--mqport The port number used by the JMS service. The default value

is 7676.

-update-resources Helps update the resources. The default value is true.

--mguser The user name for the JMS service. The default value is

admin.

--mgpassword The password for the JMS service. The default value is admin.

--property Optional attribute name/value pairs for configuring the JMS

host.

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

Examples EXAMPLE 1 Using the create-jms-host command

The following command creates a JMS host named MyNewHost:

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

Exit Status 0 command executed successfully

1 error in executing the command

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

Synopsis create-ims-resource [--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile *filename*] [--help] [--target target] --restype *type* [--enabled=*true*] [--description text] [--property (name=value)[:name=value]*] indi 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 is 4848. If set to true, uses SSL/TLS to communicate with the domain -s --secure administration server.

login command, then you need not specify the --user option on subsequent operations to this particular domain. The --passwordfile option specifies the name, including

If you have authenticated to a domain using the asadmin

--passwordfile The --passwordfile option specifies the name, including

administrative username.

the full path, of a file containing the password entries in a

The authorized domain administration server

-u --user

Name create-jms-resource – creates a JMS resource

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

--target

instance_name, which creates the resource for a particular server instance

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

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

Text providing details of the JMS resource.

Optional attribute name/value pairs for configuring the JMS resource.

You can specify the following properties for a connection factory resource:

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

--restype

--enabled

--description

--property

Application Server 9.1 Section 1: Administration Commands

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.

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.

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:

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 *indi* 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)

Synopsis create-jndi-resource [--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user]

Name create-jndi-resource – registers a JNDI resource

[--passwordfile filename] [--help]

[--target target]

--jndilookupname lookup_name --restype type --factoryclass class_name [--enabled=true]

[--description text] [--property (name=value)[:name=value]*] jndi_name

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

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	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.

The -- passwordfile option specifies the name, including the full path, of a file containing the password entries in a

--passwordfile

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option helps specify the target to which you are deploying.

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

--help

--target

• *instance name*, which creates the resource for a particular server instance

The lookup name that the external container uses.

This option is deprecated. Use --- restype instead.

The JNDI resource type. It can be topic or queue.

The class that creates the JNDI resource.

Determines whether the resource is enabled at runtime.

The text that provides details about the JNDI resource.

Optional attribute name/value pairs for configuring the resource. The following properties are available:

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.

This property specifies orb-listener-1-port

> the ORB listener port for IIOP connections that orb-listener-1 listens on.

IIOP_SSL_LISTENER_PORT This property specifies

> the ORB listener port for IIOP connections that the IIOP listener called SSL listens on.

--jndilookupname

--resourcetype

--restype

-- factoryclass

--enabled

--description

--property

IIOP_SSL_MUTUALAUTH_PORT This property specifies

the ORB listener port for IIOP connections that 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

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-jym-options - creates JVM options in the Java configuration or profiler element of the domain.xml file.

Synopsis create-jvm-options

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --target target]
[--profiler={true|false}] (jvm_option_name=jvm_option_value)
[:jvm_option_name=jvm_option_name*]
```

Description The create-jwm-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

-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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--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. Default is false.

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 4848 --target server
```

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

\\\\-Dunixlocation=/root/example:
-Dvariable=\\$HOME:-Dwindowslocation=d\\\\:\\\\\sun\\\\\appserver:
-Doption1=-value1
Command create-jvm-options executed successfully

Exit Status 0 command executed successfully

1 error in executing the command

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

Name create-lifecycle-module – adds a lifecycle module

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

-I --interactive

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	classname	This is the fully qualified name of the startup class.
	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.

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

The HTTP/S port for administration. This is the port to -p --port which you should point your browser in order to manage the

domain. For example, http://localhost:4848.

If set to true (default), only the required password options

The default port number is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

administration server.

The authorized domain administration server -u --user

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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

Displays the help text for the command.

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 indicates where this module is actually located if it is not under applications-root.

This option represents an integer value that can be used to force the order in which deployed lifecycle modules are

--help

--target

--classpath

--loadorder

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --ruleenabled =true|false]
[--ruledescription description] [--action action-mbean-name]
--eventtype event-type [--eventloglevel log-level
[--recordevent=true|false] [ --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.

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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--heln

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.

Valid values are:

- cluster
- lifecycle
- log
- monitor

- notification
- timer
- trace

--eventloglevel

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

Valid values are:

- FINEST
- FINER
- FINE
- CONFIG
- INFO
- WARNING
- SEVERE
- OFF

-- recordevent

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

--eventdescription

A description of the event.

--eventproperties

The properties defined for the event. Different events have different properties. If you do not specify a value for some properties, defaults are used. The following properties and their values are identified for each event type:

name

Notifies when the GMS starts, stops, or reports failure of a server instance.

Values: start, stop, fail

Event type: cluster

serverName

Specifies the server instances about which notifications are given.

Values: A comma-separated list of server instance names, or * for all server instances.

Event type: cluster

name

Specifies a server life cycle event.

Values: ready, shutdown, termination.

Event type: lifecycle

loggerNames

(optional) Notifies when the specified loggers write messages to the server log.

Values: A comma-separated list of logger names, or * for all loggers, which is the default.

Event type: log

level

(optional) Notifies when messages of the specified level are written to the server log.

Values: A comma-separated list of log levels.

Event type: log

observedMbean

Specifies the name of the monitored MBean. Either this property or observedObject must be specified.

Values: A name attribute of a user-defined MBean, or a JMX ObjectName for a system MBean.

Event type: monitor

observedObject

Specifies the name of the monitored MBean. Either this property or observedMbean must be specified.

Values: An object-name attribute of a user-defined MBean, or a JMX ObjectName for a system MBean.

Event type: monitor

observedAttribute

Specifies the monitored attribute of the monitored MBean.

Values: An MBean Attribute name.

Event type: monitor

monitorType

The type of monitoring of the attribute.

Values: CounterMonitor, GaugeMonitor, StringMonitor

Event type: monitor

granularityPeriod

(optional) Specifies the granularity at which the monitoring data should be collected, in seconds.

Values: any numerical value representing the number of seconds of data monitoring.

Event type: monitor

notifyMatch

Specifies that the attribute value must match the stringToCompare value. Either this property or notifyDiffer is required if the monitor type is StringMonitor.

Values: true or false

Event type: monitor

notifyDiffer

Specifies that the attribute value must not match the stringToCompare value. Either this property or notifyMatch is required if the monitor type is StringMonitor.

Values: true or false

Event type: monitor

stringToCompare

Specifies the value to which the attribute value is compared. Required if the monitor type is StringMonitor.

Event type: monitor

numberType

Specifies the type of the numeric value being monitored. Required if the monitor is of type CounterMonitor or GaugeMonitor.

Values: byte, double, float, int, long, short

Event type: monitor

differenceMode

Specifies the difference mode flag value common to all observed MBeans. Required if the monitor is of type CounterMonitor or GaugeMonitor.

Values: true or false

Event type: monitor

initThreshold

Specifies a value above which notification occurs. Required if the monitor is of type CounterMonitor.

Event type: monitor

offset

(optional) Specifies that the event should be re-triggered when the initThreshold value plus this offset value is reached. Applicable if the monitor is of type CounterMonitor.

Event type: monitor

modulus

(optional) Specifies the modulus value common to all observed MBeans. Applicable if the monitor is of type CounterMonitor.

Event type: monitor

highThreshold

Specifies the upper limit of the range within which notification occurs. Required if the monitor is of type GaugeMonitor.

Event type: monitor

lowThreshold

Specifies the lower limit of the range within which notification occurs. Required if the monitor is of type GaugeMonitor.

Event type: monitor

sourceMBean

Specifies a custom MBean that implements the JMX NotificationEmitter interface. Either this property or sourceObjectName must be specified.

Values: name of an Mbean

Event type: notification

sourceObjectName

Specifies a custom MBean that implements the JMX NotificationEmitter interface. Either this property or sourceMBean must be specified.

Values: object-name of Mbean

Event type: notification

type

(optional) Specifies the notification type. If this property is specified, the action of the parent management rule is performed only if the notification type emitted is same as this property's value.

Event type: notification

dateString

Begins notification at the specified date and time.

Values: Input format determined by the pattern property

Event type: timer

pattern

(optional) Specifies the date and time input format. The default is mm/dd/yyyy hh:mm:ss.

Event type: timer

period

(optional) Notification repeats at the specified time interval in miliseconds.

Event type: timer

numberOfOccurrences

(optional) Specifies the number of times notification occurs.

Event type: timer

message

(optional) Specifies a message that is delivered as part of timer notification.

Event type: timer

name

Notifies at the specified trace point.

 $Values: web_component_method_entry, web_component_method_exit, \\ ejb_component_method_entry, ejb_component_method_exit, \\ request_end$

Event type: trace

ipAddress

Specifies the IP address for which trace notifications are sent.

Values: An IP address

Event type: trace

callerPrincipal

Specifies the caller principal for which trace notifications are sent.

Event type: trace

componentName

Specifies the component name for which trace notifications are sent.

Event type: trace

--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

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-lifecycle-module(1), list-lifecycle-modules(1)

Name create-mbean – creates and registers a custom MBean

Synopsis create-mbean

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --name name]
[--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.

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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--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 <code>appserver_install_dir/domains_dir/applications/mbeans</code> 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

```
asadmin> create-mbean --user admin --passwordfile filename.txt
--objectname "user:type=com.example.Foo" 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

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

This example assumes that there is a target with name cluster1, comprised of server instances server1, server2).

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={true|false}][ --echo={true|false} ]
          [ --interactive={true|false} ] [ --host host]
          [--port port] [--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 precedes the long option name. Short options have one dash whereas long options have two dashes.

-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
-Iinteractive	If set to true (default), only the required password options are prompted.
-Hhost	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 is 4848.

If --4.4- American CCI /TI C.4- -- many

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

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.

The --passwordfile option specifies the name, including the full path, 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.

-s --secure

-u --user

--passwordfile

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

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This operand is valid in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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

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

classname

--help

--target

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 hefore-content or after-content. The default value is after-content.

responseauthsource

The auth-source attribute defines a requirement for message-layer sender authentication (e.g. username password) or content authentication (e.g. digital signature) to be applied to response messages. Possible values are sender or content. When this option is not specified, source authentication of the response is not required.

responseauthrecipient

The auth-recipient attribute defines a requirement for message-layer authentication of the receiver of the response message to its sender (e.g. by XML encryption). Possible values are before-content or after-content. The default value is after-content.

isdefaultprovider

The default-provider attribute is used to designate the provider as the default provider (at the layer) of the type or types identified by the providertype argument. There is no default associated with this option.

property

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

Operands provider_name

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

Examples EXAMPLE 1 Using create-message-security-provider

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

```
asadmin> create-message-security-provider --user admin
```

- --passwordfile pwd file
- --classname com.sun.enterprise.security.jauth.ClientAuthModule
- --providertype client mySecurityProvider

Exit Status 0

command executed successfully

1

error in executing the command

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

Name create-node-agent – creates a node agent

Synopsis create-node-agent

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --agentdir nodeagent_path] [--agentport port_number]
[--agentproperties (name=value)[:name=value]*]
[--savemasterpassword={true|false}] [nodeagent_name]
```

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

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

The DAS connection options (host, port, user) identify the agent's initial target domain. The DAS does not need to be running when the node agent is being created. When the node agent is started, the agent attempts to contact the DAS to join the domain.

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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

-heln

Displays the help text for the command.

--agentdir

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

--agentport

The port on which the node agent's JMX connector listens and accepts requests. If not specified, then a random unused port is chosen.

--agentproperties

The following agent properties are available:

listenaddress

The address used by the JMX connector to listen for requests or notifications. The default is 0.0.0.0.

remoteclientaddress

The address used by DAS to connect to the Node Agent. The default is the hostname of the server.

loglevel

The initial log level at which messages are logged. The default is INFO.

--savemasterpassword

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

Operands *nodeagent_name*

The name of the node agent must be unique in the domain. If not specified, the *nodeagent_name* defaults to the machine's host name. Do not use any reserved words or characters in the node agent name. For more information on these restrictions, see the asadmin help page (enter asadmin --help at the command prompt).

Examples EXAMPLE 1 Using create-node-agent

```
asadmin>create-node-agent --host host1 --port 4848
--user admin1 --passwordfile password.txt nodeagent1
Node Agent nodeagent1 created.
```

The node agent nodeagent1 was created in the default <code>install_dir/nodeagents</code> directory.

Exit Status 0

0 command executed successfully

1 error in executing the command

See Also delete-node-agent(1), list-node-agent(1), start-node-agent(1), stop-node-agent(1)

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

```
Synopsis create-node-agent-config
          [--terse={true|false}][ --echo={true|false} ]
          [ --interactive={true|false} ] [ --host host]
          [--port port] [--secure| -s ] [ --user admin_user]
          [--passwordfile filename] [--help]
           nodeagent_name
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> This command creates a node agent placeholder on the Domain Administration Server. You can create the placeholder before creating the node agent's directory structure on the local machine using the create-node-agent command. The create-node-agent-config command supports the offline configuration scenario where administrators define server instances in advance of creating the node agents on remote machines.

Options	5
---------	---

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser

option on subsequent operations to this particular domain.

--passwordfile

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

Examples EXAMPLE 1 Using create-node-agent-config

--help **Operands** nodeagent_name

asadmin> create-node-agent-config --user admin1 --passwordfile filename nodeagent1

Command create-node-agent-config executed successfully.

Application Server 9.1 Section 1: Administration Commands

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

See Also delete-node-agent-config(1), create-node-agent(1)

Name create-password-alias – creates a password alias

Synopsis create-password-alias

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] 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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	The passwordfile option specifies the name, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The name of the alias password as it appears in domain.xml file.

--help

Operands -aliasname

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

asadmin> create-password-alias --user admin --passwordfile /home/password.txt --interactive=true imspassword-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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser

option on subsequent operations to this particular domain.

--passwordfile

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Determines whether the resource is enabled at runtime.

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.

--help

--enabled

--target

•	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 valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

--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

 ${\it asadmin}{\gt create-persistence-resource} \ {\it --user} \ {\it admin} \ {\it --passwordfile} \ passwords.txt \ {\it --connection poolid} \ testPool \ testPersistence$

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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

--target

• *instance_name*, which creates the profiler for a particular server instance

--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.

Name/value pairs of provider specific attributes. --property

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

Created Profiler with id = sample profiler

Where: sample profiler is the profiler created.

Exit Status 0 command executed successfully

> 1 error in executing the command

See Also delete-profiler(1)

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

```
Synopsis create-resource-adapter-config
          [--terse={true|false}][ --echo={true|false} ]
          [ --interactive={true|false} ] [ --host host]
          [--port port] [--secure| -s ] [ --user admin_user]
          [--passwordfile filename] [--help]
```

[--threadpoolid threadpool] [--property (property name=value)[:name=value]*]

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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser

option on subsequent operations to this particular domain.

--passwordfile

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option has been deprecated.

The threadpool ID from which the work manager gets the thread. This option takes only one threadpool ID.

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 (:).

--help

--target

--threadpoolid

--property

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

 $\hbox{\it --passwordfile passwords.txt --property foo=bar --threadpoolid mycustomerthreadpool}$

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-resource-ref – creates a reference to a resource

Synopsis create-resource-ref

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
 [ --target target]
 [--enabled=true] reference_name
```

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

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

This command is supported in remote mode only.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target for which you are creating the resource reference. Valid targets are

 server, which creates the resource reference for the default server instance. This is the default target.

--help

--target

- *cluster_name*, which creates the resource reference for every server instance in the cluster
- instance_name, which creates the resource reference for the named unclustered server instance

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

--enabled

Indicates whether the resource should be enabled. This value will take effect only if the resource is enabled at the global level. The default is true.

Operands reference_name

The name or JNDI name of the resource.

Examples EXAMPLE 1 Using the create-resource-ref command

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

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

Exit Status 0 command executed successfully

1 error in executing the command

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

Name create-service – configures the starting of a DAS or node agent on an unattended boot.

Synopsis create-service --passwordfile passwordfile

[--echo={true | false}][--terse={true | false}][--name servicename] [--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 svccfq, 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 --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.

-e--echo

Setting to true will echo the command line statement on the standard output. Default is false.

1

-t --terse Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is Indicates the name of the service and overrides the default, if --name present. Specifies whether the service pertains to DAS or node agent. --type 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. --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. Exit Status 0 command executed successfully

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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.

-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
-Iinteractive	If set to true (default), only the required password options are prompted.
-Hhost	The machine name where the domain administration server is running. The default value is localhost.
-pport	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 is 4848.
-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option is valid only in domains that are configured to support clusters, such as domains that are created with the

--help

--target

cluster profile or the enterprise profile.. 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

Optional 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 <i>http-listener</i> , <i>iiop-listener</i> , or <i>iiop-service</i> . When the type is <i>iiop-service</i> , 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 <i>tokenname:nickname</i> . For this property, the <i>tokenname</i> : is optional.
ssl2enabled	Set this property to <i>true</i> to enable SSL2. The default value is <i>false</i> . If both SSL2 and SSL3 are enabled for a virtual server, the server tries SSL3 encryption first. In the event SSL3 encryption fails, the server then tries SSL2 encryption.
ssl2ciphers	A comma-separated list of the SSL2 ciphers to be used. Use the prefix + to enable or – to disable a particular cipher. Allowed values are: rc4, rc4export, rc2, rc2export, idea, des, and desede3. If no value is specified, all supported ciphers are assumed to be enabled.

Property	Definition	
ssl3enabled	Set this property to <i>false</i> to disable SSL3. The default value is <i>true</i> . If both SSL2 and SSL3 are enabled for a virtual server, the server tries SSL3 encryption first. In the event SSL3 encryption fails, the server then tries SSL2 encryption.	
tlsenabled	Set this property to <i>false</i> to disable TLS. The default value is <i>true</i> It is good practice to enable TLS, which is a more secure version of SSL.	
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_and SSL_RSA_WITH_NULL_SHA. If no value is specified, all supported ciphers are assumed to be enabled.	t_128_SHA,
tlsrollbackenabled	Set to <i>true</i> (default) to enable TLS rollback. TLS rollback should be enabled for Microsoft Internet Explorer 5.0 and 5.5. This option is only valid when -tlsenabled= <i>true</i> .	
clientauthenabled	Set to <i>true</i> if you want SSL3 client authentication performed on every request independent of ACL-based access control. Default value is <i>false</i> .	

Operands listener_id

The ID of the 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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--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.

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 4848
--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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser

option on subsequent operations to this particular domain.

--passwordfile

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

--target

		 cluster_name, which creates the threadpool for every server instance in the cluster
		• <i>instance_name</i> , which creates the threadpool for a particular server instance
	maxthreadpoolsize	Maximum number of threads in the threadpool servicing requests in this queue. This is the upper bound on the number of threads that exist in the threadpool.
	minthreadpoolsize	Minimum number of threads in the threadpool servicing requests in this queue. These are created up front when the threadpool is instantiated.
	idletimeout	Idle threads are removed from the pool after this time.
	workqueues	Identifies the total number of work queues serviced by this threadpool.
Operands	threadpool_id	an ID for the work queue; for example, thread-pool-1, thread-pool-2, etc.
Examples	EXAMPLE 1 Using create-threadpool	Command
	asadmin> create-threadpooluser admin1passwordfile password.txtmaxthreadpoolsize 100minthreadpoolsize 20idletimeout 2workqueues 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 --rulefilelocation rulefile_location [--enabled={true | false] [--applyto=request | response | both] 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 location of the file to do the transformation. Only XSLT files -rulefilelocation are allowed. Default location is instance dir/generated/xml/application name or module name/XSLTfilename -t --terse Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false. -e --echo Setting to true will echo the 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 is 4848. If set to true, uses SSL/TLS to communicate with the domain -s --secure administration server. The authorized domain administration server -u --user 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, including the full path, 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

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

Displays the help text for the command.

if set to true, enables the web service endpoint.

name of the web service operation

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.

name of the transformation rule being created.

uppercase letters.

Operands transformation-rule-name

--help

--enabled

--applyto

-operationname

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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.

--help

--target

- *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 valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

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.

A comma-separated (,) list of HTTP listener IDs. Required only for a virtual server that is not the default virtual server.

The standalone web module associated with this virtual server by default.

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.

Name of the file where log entries for this virtual server are to be written. By default, this is the server log.

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.

--hosts

--httplisteners

--defaultwebmodule

--state

--logfile

--property

Property	Definition
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.
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 \$[\$1AS_HOME]/domains/domain

n1/config/defaul

Property	Definition
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></sun-web-app>
	<pre><pre><pre><pre><pre><pre><pre>property name="allowLinking" value="[true false]"/></pre></pre></pre></pre></pre></pre></pre>
	The default value is true.
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.

Property	Definition	
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.	
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().gr 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.	etHostName())
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().get 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.	etHostName())

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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]
[--passwordfile filename] [--help]
[--target target]
indi_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 is 4848.

-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, including

the full path, 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:

210

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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. 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

JNDI name of the administered object to be deleted.

--help

--target

Operands *jndi_name*

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-application-ref – removes a reference to an application

Synopsis delete-application-ref

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --target target]
[--cascade=false] reference_name
```

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

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

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

This command is supported in remote mode only.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target from which you are removing the application reference. Valid values are

 server, which removes the application reference from the default server instance server and is the default value

--help

--target

- *cluster_name*, which removes the application reference from every server instance in the cluster
- instance_name, which removes the application reference from the named unclustered server instance

--cascade

For a connector module, indicates whether the resources dependent on the module should also be recursively deleted. The default is false. The connector module can be either a stand-alone RAR file or a module within an EAR file.

Operands reference_name

The name of the application or module, which can be a Java EE application module, Web module, EJB module, connector module, application client module, or lifecycle module.

Examples EXAMPLE 1 Using the delete-application-ref command

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

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

Exit Status 0 command executed successfully

l error in executing the command

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

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

Synopsis delete-audit-module

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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 is 4848.

-s --secure If set to true, uses SSL/TLS to communicate with the domain

administration server.

The authorized domain administration server -u --user

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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target on which you are deleting the audit module. Valid values are

- server, which deletes the audit module for the default server instance server and is the default value
- configuration_name, which deletes the audit module for the named configuration
- cluster_name, which deletes the audit module for every server instance in the cluster
- instance_name, which deletes the audit module for a particular server instance

name of the audit module to be deleted.

--help

--target

Operands *audit_module_name*

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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.

		7
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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.
		TTI 1 C 1 1

The default port number is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target on which you are deleting the authentication realm. This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. Valid values are

- server, which deletes the realm for the default server instance server and is the default value
- configuration_name, which deletes the realm for the named configuration
- *cluster_name*, which deletes the realm for every server instance in the cluster
- instance_name, which deletes the realm for a particular server instance

name of this realm.

--help

--target

Operands *auth_realm_name*

Examples EXAMPLE 1 Using delete-auth-realm

 $\verb|asadmin>| \textbf{delete-auth-realm}| \textbf{--user}| \textbf{admin1}| \textbf{--passwordfile}| \textbf{password.txt}|$

--host pigeon --port 5001 db

Command delete-auth-realm executed successfully

Where db is the authentication realm deleted.

Exit Status 0 command executed successfully

1 error in executing the command

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

Name delete-cluster – deletes a cluster

Synopsis delete-cluster

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --autohadboverride ={true|false}]
cluster name
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide

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

> If a standalone cluster is deleted (that is, the cluster's configuration name is *cluster_name* - config and no other clusters or unclustered instances refer to this configuration), then its standalone configuration is automatically deleted. If HADB is installed and is being used,, the HADB database associated with a cluster can also be deleted when the cluster is deleted, depending upon the cluster's autohadb setting and whether you override it using this command's autohadboverride 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

-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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--autohadboverride

This option is valid only if the HADB software is installed. The autohadboverride option determines whether to override the cluster's setting for the autohadb option. When the cluster was created, the autohadb option was set to signal whether the HADB database associated with the cluster would be started, stopped, or deleted when the cluster was started, stopped, or deleted. You can override this value by using the autohadboverride option. If autohadboverride is set to true, the HADB database is deleted when the cluster is deleted. If set to false, the HADB database is not deleted when the cluster is deleted. If the

autohadboverride option is not set, the default is to use the cluster's autohadb setting.

Operands *cluster_name* The name of

The name of the cluster to be deleted.

Examples EXAMPLE 1 Using the delete-cluster command

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

asadmin> delete-cluster --user admin1
--passwordfile passwords.txt MyCluster

Command delete-cluster executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

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

Name delete-config – deletes an existing configuration

Synopsis delete-config

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] configuration_name

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

	used to create new standalone configurations.	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.

The -- passwordfile option specifies the name, including

the full path, of a file containing the password entries in a

--passwordfile

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The name of the configuration you are deleting.

Examples EXAMPLE 1 Using the delete-config command

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

Exit Status 0 command executed successfully

1 error in executing the command

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

--help

Operands configuration_name

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

Synopsis delete-connector-connection-pool

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

[--cascade =false] connector_connection_pool_name

 $\textbf{Description} \quad \text{The delete-connector-connection-pool command removes the connector connection}$

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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--help Displays the help text for the command.

--target This option is deprecated.

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

--cascade

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

EXAMPLE 1 Using the delete-connector-connection-pool command (Continued)

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

-H --host

-p --port

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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 *indi_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. Setting to true will echo the command line statement on the -e --echo standard output. Default is false. -I --interactive If set to true (default), only the required password options are prompted.

The machine name where the domain administration server

The HTTP/S port for administration. This is the port to which you should point your browser in order to manage the

is running. The default value is localhost.

domain. For example, http://localhost:4848.

The default port number is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

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, including

> the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

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.

--help

--target

• *instance_name*, which deletes the connector resource from a specified server instance.

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 a domain whose profile is the developer profile.

```
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 a domain whose profile is the cluster profile.

```
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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option is deprecated.

Specifies the name of the connector connection pool to which the security map that is to be deleted belongs.

name of the security map to be deleted.

--help

--target

--poolname

Operands *security_map_name*

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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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.

The machine name where the domain administration server -H --host

is running. The default value is localhost.

The HTTP/S port for administration. This is the port to -p --port

which you should point your browser in order to manage the

domain. For example, http://localhost:4848.

The default port number is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

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, including

> the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

--target

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

Operands *indi_name* the JNDI name of this resource.

Examples EXAMPLE 1 Using the delete-custom-resource command

 $\verb|asadmin>| \textbf{delete-custom-resource}| \textbf{--user}| \textbf{admin}| \textbf{--passwordfile}| \textbf{passwords.txt}| \textbf{sample_custom_resource}|$

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 <code>install_dir/domains</code>

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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]
[--passwordfile filename] [--help]
[--target target]

1 cornama

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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This is the name of the target on which the command operates. This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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

This is the name of file user to be deleted.

--help

--target

Operands username

Examples EXAMPLE 1 Using the delete-file-user command

asadmin> delete-file-user --user admin --passwordfile passwords.txt --host pigeon --port 5001 samp

Command delete-file-user executed successfully

Exit Status 0 command executed successfully

1 error in executing the command

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

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

Synopsis delete-http-health-checker

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --config config_name]
target
```

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> This command deletes the health checker from a load balancer configuration. A health checker is unique for the combination of target and load balancer configuration.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The load balancer configuration from which you delete the health-checker.

Specifies the target from which you are deleting the health checker.

Valid values are:

--help

--config

Operands target

- *cluster_name*, which deletes the health checker that was monitoring all instances in the cluster.
- *stand-alone_instance_name*, which deletes the health checker that was monitoring this stand-alone instance.

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

asadmin> delete-http-health-checker --user admin

--passwordfile password.txt --config mycluster-http-lb-config mycluster

Command delete-http-health-checker executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

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

Name delete-http-lb – deletes a load balancer

Synopsis delete-http-lb

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help]

load balancer name

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

Use the delete-http-lb command to delete a physical load balancer.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The name of the load balancer to be deleted.

Examples EXAMPLE 1 Using the delete-http-lb-config command

asadmin> delete-http-lb --user admin --passwordfile password.txt mylb Command delete-http-lb executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also create-http-lb(1), list-http-lbs(1)

--help

Operands *load_balancer_name*

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

Synopsis delete-http-lb-config

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
config_name
```

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> Use the delete-http-lb-config command to delete a load balancer configuration. The load balancer configuration must not reference any clusters or server instances enabled for load balancing. In addition, the load balancer configuration must not be referenced by any physical load balancers.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The name of the load balancer configuration to delete. The configuration must not reference any clusters or server instances enabled for load balancing, or be used by any physical load balancers.

Examples EXAMPLE 1 Using the delete-http-lb-config command

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

-xamples example i Osing the delete-intip-

--help

Operands *config_name*

Exit Status 0 command executed successfully

1 error in executing the command

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

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

Synopsis delete-http-lb-ref

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
  --config config_name | --lbname load_balancer_name
[--force=false] target
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> Use the delete-http-lb-ref command to remove a reference to a cluster or stand-alone server instance from a load balancer configuration or load balancer. So that you do not interrupt user requests, make sure the standalone server instance or all server instances in the cluster are disabled before you remove them from the load balancer configuration. If the force option is set to true, the references are deleted even if server instances or clusters are enabled.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies which load balancer configuration to delete cluster and server instance references from.

--help

--config

Specify either a load balancer configuration or a load balancer. Specifying both results in an error. -- 1 bname Specifies the load balancer to delete cluster and server instance references from. Specify either a load balancer configuration or a load balancer. Specifying both results in an error. If force is set to true, then the references are deleted even if --force there are currently enabled applications or instances. The default is false. **Operands** target Specifies which cluster or instance to remove from the load balancer. Valid values are: cluster_name, which specifies that requests for this cluster will no longer be handled by the load balancer. stand-alone_instance_name, which specifies that requests for this stand-alone instance will no longer be handled by the load balancer. **Examples** EXAMPLE 1 Using the delete-http-lb-ref command asadmin> delete-http-lb-ref --user admin --passwordfile file --config mycluster-http-lb-config cluster2 Command delete-http-lb-ref executed successfully.

command executed successfully

error in executing the command

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

Exit Status 0

1

Name delete-http-listener – removes an HTTP listener

Synopsis delete-http-listener

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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.

The machine name where the domain administration server -H --host

is running. The default value is localhost.

The HTTP/S port for administration. This is the port to -p --port

which you should point your browser in order to manage the

domain. For example, http://localhost:4848.

The default port number is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

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, including

> the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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

--help

--target

• *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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]
[--passwordfile filename] [--help]
[--target server]
listener id

 $\textbf{Description} \quad \text{The delete-iiop-listener command removes the specified IIOP listener. This command is} \quad$

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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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

--help

--target

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
 instance name
```

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

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

Options

-t --terse

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.

-e --echo

Setting to true will echo the 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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

Operands *instance_name* name of the instance to be deleted.

Examples EXAMPLE 1 Using delete-instance:

asadmin> delete-instance --user admin
--passwordfile passwords.txt --host pigeon
--port 4848 instance2

Command delete-instance executed successfully

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --target target]
jndi_name
```

Description The delete-javamail-resource command removes the specified JavaMail session resource. Ensure that you 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 is 4848.

-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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--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 valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

Operands *indi_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
```

EXAMPLE 1 Using the delete-javamail-resource command (Continued)

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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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.

> 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.

	1 1	,
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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.

This option is deprecated.

The name of the JDBC resource to be removed.

--help

--cascade

--target

Operands connection poolid

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

asadmin delete-jdbc-connection-pool --user admin --passwordfile passwords.txt --host localhos

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.

1

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --target target]
jndi_name
```

Description The delete-jdbc-resource command removes a JDBC resource. Ensure 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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--target

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

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 *indi_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 a domain whose profile is the developer profile.

asadmin> delete-jdbc-resource --user admin --passwordfile passwords.txt jdbc/DerbyPool

```
EXAMPLE 1 Using the delete-jdbc-resource command (Continued)

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 a domain whose profile is the cluster profile.

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
```

270

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

Name delete-jmsdest – removes a JMS destination

Synopsis delete-imsdest

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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.

Setting to true will echo the command line statement on the -e --echo

standard output. Default is false.

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

are prompted.

The machine name where the domain administration server -H --host

is running. The default value is localhost.

The HTTP/S port for administration. This is the port to -p --port

which you should point your browser in order to manage the

domain. For example, http://localhost:4848.

The default port number is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

administration server.

The authorized domain administration server -u --user

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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

--target

• *instance_name*, which deletes the physical destination from a particular server instance

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

-T -- desttype

The type of the JMS destination. Valid values are topic and

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:

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

Exit Status 0

command executed successfully

1

error in executing the command

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

Name delete-jms-host – removes a JMS host

Synopsis delete-ims-host

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [--target target] jms_host_name

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

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

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.

The machine name where the domain administration server -H --host

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 is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

administration server.

The authorized domain administration server -u --user

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.

The --passwordfile option specifies the name, including --passwordfile

> the full path, 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.

274

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target from which you are deleting the JMS host. Valid targets are

- server, which deletes the JMS host from the default server instance and is the default value
- configuration_name, which deletes the JMS host from the named configuration
- cluster_name, which deletes the JMS host from every server instance in the cluster
- instance_name, which deletes the JMS host from a particular server instance

--help

--target

This option is valid only in domains that are configured to support clusters, such as domains that are created with the

cluster profile or the enterprise profile.

-update-resources Helps update the resources. The default value is true.

Operands *jms_host_name* The name of the host to be deleted.

Examples EXAMPLE 1 Using the delete-jms-host command

The following command deletes the JMS host namedMyNewHost.

asadmin> delete-jms-host --user admin1
--passwordfile passwords.txt MyNewHost

Command delete-jms-host executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

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

Name delete-jms-resource – removes a JMS resource

Synopsis delete-jms-resource

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [-- target target] jndi_name

Description The delete-jms-resource command removes the specified JMS resource. Ensure that you remove all references to this resource before executing this command. This command is supported in remote mode only.

	supported in remote mode only	•
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

administration server.

The authorized domain administration server -u --user

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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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 valid only in domains that are configured to support clusters, such as domains that are created with the

--help

--target

cluster profile or the enterprise profile.

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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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.

You must remove all associations to the JNDI resource before you execute this command.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, of a file containing the password entries in a

uppercase letters.

specific format. The entry for the password must have the AS ADMIN prefix followed by the password name in

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

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

--help

--target

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 : 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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --target target]
[ --profiler={true|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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--heln

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 valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

--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 4848 "\\-Dtmp=sun"
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 4848 "\\-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-options(1)

Name delete-lifecycle-module – removes the lifecycle module

Synopsis delete-lifecycle-module

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile *filename*] [--help]

[--target target]
module_name

Description The delete-lifecycle-moduleremoves 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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--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.

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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

The name of the management rule.

Operands rule_name

--help

-- target

Examples EXAMPLE 1 using delete-management-rule

```
asadmin> delete-management-rule --user admin
--passwordfile adminpassword.txt --target myinstance myRule1
```

290

EXAMPLE 1 using delete-management-rule (Continued)

Command delete-management-rule executed successfully

Exit Status 0 command executed successfully

1 error in executing the command

See Also delete-lifecycle-module(1), list-lifecycle-modules(1)

Name delete-mbean – deletes a custom MBean.

Synopsis delete-mbean

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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.

-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
-Iinteractive	If set to true (default), only the required password options are prompted.
-Hhost	The machine name where the domain administration server is running. The default value is localhost.
-pport	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 is 4848.
-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
-uuser	The authorized domain administration server administrative username.
	If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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.

Identifies a custom MBean by name. The default name is the MBean's implementation class name.

--help

--target

Operands - 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={true|false}][ --echo={true|false} ]
          [ --interactive={true|false} ] [ --host host]
          [--port port] [--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 preceds the long option name. Short options have one dash whereas long options have two dashes.

-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
-Iinteractive	If set to true (default), only the required password options are prompted.
-Hhost	The machine name where the domain administration server is running. The default value is localhost.
-pport	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 is 4848.
-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.

-u --user

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

--help

This operand is valid in domains that are configured to --target support clusters, such as domains that are created with the cluster profile or the enterprise profile. Specifies the target to which you are deploying. Valid values are • server, which deploys the component to the default server instance server and is the default value domain, which deploys the component to the domain. • *cluster_name*, which deploys the component to every server instance in the cluster. • *instance_name*, which deploys the component to a particular sever instance. The message-layer from which the provider has to be --laver deleted. The default value is SOAP. **Operands** *provider_name* The name of the provider used to reference the provider-config element. **Examples** EXAMPLE 1 Using delete-message-security-provider The following example shows how to delete a message security provider for a client. asadmin> delete-message-security-provider --user admin --layer SOAP mySecurityProvider Exit Status 0 command executed successfully 1 error in executing the command **See Also** create-message-security-provider(1), list-message-security-providers(1)

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

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

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

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

Options -t--terse Indicates that any output data must be very concise, typically

avoiding human-friendly sentences and favoring

well-formatted data for consumption by a script. Default is

false.

Setting to true will echo the command line statement on to -e--echo

the standard output. Default is false.

-I--Interactive If set to true (default), only the required options are

prompted.

Like a Domain Administration Server (DAS), each node --agentdir

agent resides in a top level directory named

agentdir/nodeagent_name. If specified, the path must be accessible in the filesystem. If not specified, defaults

toinstall_dir/nodeagents directory.

Operands *nodeagent_name* The name of the node agent to be deleted.

Examples EXAMPLE 1 Using delete-node-agent

asadmin> delete-node-agent nodeagent1 Node Agent nodeagent1 deleted.

Where: nodeagent1, residing in the default <code>install_dir/nodeagents</code> directory, is deleted together with its directory structure. Please note that at this point nodeagent1 references still exist in domain.xml. Use the delete-node-agent-config command to complete the removal process.

Exit Status 0 command executed successfully

> 1 error in executing the command

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

Name delete-node-agent-config – removes a node agent from a domain

Synopsis delete-node-agent-config

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
nodeagent_name
```

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

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

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

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

Operands nodeagent_name

Examples EXAMPLE 1 Using delete-node-agent-config

asadmin> delete-node-agent-config --user admin1 --passwordfile filename nodeagent1

 ${\tt Command\ delete-node-agent-config\ executed\ successfully.}$

Exit Status 0 command executed successfully

1 error in executing the command

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

Name delete-password-alias – deletes a password alias

Synopsis delete-password-alias

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This is the name of the substitute password as it appears in domain.xml.

Examples EXAMPLE 1 Using delete-password-alias command

--help

Operands -aliasname

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={true|false}][ --echo={true|false} ]
          [ --interactive={true|false} ] [ --host host]
          [--port port] [--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. Ensure that you remove all associations to this resource and then execute this command.

_	-	•		
(1	pt	10	nc	

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.			
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.			
	-Iinteractive	If set to true (default), only the required password options are prompted.			
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.			
	-pport	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 is 4848.			
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.			
	-uuser	The authorized domain administration server administrative username.			
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.			
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target from which you are deleting a persistence resource. This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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.

--help

--target

- *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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
 [ --target target_name]
```

Description The delete-profiler command 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.

	11	,
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

- --help
- --target

• *instance_name*, deletes the profiler element for a particular server instance

Examples EXAMPLE 1 Using delete-profiler

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

Exit Status 0 command executed successfully

1 error in executing the command

See Also create-profiler(1)

Name delete-resource-adapter-config – deletes the resource adapter configuration

Synopsis delete-resource-adapter-config

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

raname

 $\textbf{Description} \quad \text{The delete-resource-adapter-config command deletes the configuration information} \\$

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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--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 ral

Command delete-resource-adapter-config executed successfully

Exit Status 0 command executed successfully

1 error in executing the command

 $\textbf{See Also} \quad create-resource-adapter-config(1), list-resource-adapter-configs(1)$

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

Synopsis delete-resource-ref

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --target target]
reference_name
```

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

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

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

This command is supported in remote mode only.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target from which you are removing the resource reference. Valid values are

 server, which removes the resource reference from the default server instance server and is the default value

--help

--target

- *cluster_name*, which removes the resource reference from every server instance in the cluster
- instance_name, which removes the resource reference from the named unclustered server instance

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

Operands reference_name

The name or JNDI name of the resource.

Examples EXAMPLE 1 Using the delete-resource-ref command

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

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

Exit Status 0 command executed successfully

1 error in executing the command

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

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

Synopsis delete-ssl

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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.

-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
-Iinteractive	If set to true (default), only the required password options are prompted.
-Hhost	The machine name where the domain administration server is running. The default value is localhost.
-pport	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 is 4848.
-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
-uuser	The authorized domain administration server administrative username.
	If you have authenticated to a domain using the asadmin login command, then you need not specify theuser

option on subsequent operations to this particular domain.

--passwordfile

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This operand is valid in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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.

--help

--target

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.

The type of service or listener for which the SSL is deleted. The type can be *http-listener*, *iiop-listener*, or *iiop-service*.

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*.

Operands *listener_id*

--type

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)

318

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

Synopsis delete-system-property

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--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.

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 4848
--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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile *filename*] [--help] [--target target_name] threadpool_id

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

_								
()	pti	ınr	١c	_ +	 +	α r	~ C	Δ

Indicates that any output data must be very concise, typically

avoiding human-friendly sentences and favoring

well-formatted data for consumption by a script. Default is

false.

-e --echo

Setting to true will echo the 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 is 4848.

-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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

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

--help

--target

Operands threadpool_id

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}

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

transformation-rule-name

Description Deletes an XSLT transformation rule of a given web service.

Options --webservicename Name of the deployed webservice.

-t -- terse Indicates that any output data must be very concise, typically

avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is

false.

-e --echo Setting to true will echo the 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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--help

Operands *transformation-rule-name*

Displays the help text for the command.

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

 $\textbf{See Also} \quad create-transformation-rule (1), list-transformation-rules (1)$

Name delete-virtual-server – removes a virtual server

Synopsis delete-virtual-server

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]
[--passwordfile filename] [--help]
[--target server]
virtual server id

 $\textbf{Description} \quad \text{The delete-virtual-server command removes the virtual server with the specified virtual} \\$

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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

--target

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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]
[--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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--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. In a domain whose profile is the cluster profile or the enterprise profile, 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 valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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

A comma-separated list of library JAR files. Specify the library JAR files by their relative or absolute paths. Specify relative paths relative to *instance-root*/lib/applibs. The libraries are made available to the application in the order specified.

--target

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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. In a domain whose profile is the cluster profile or the enterprise, 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. In a domain whose profile is the cluster profile or the enterprise, 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, which is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. To use this example in a domain that is not configured to support clusters, 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.

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

This example uses the --target option, which is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. To use this example in a domain that is not configured to support clusters, 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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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 -tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.

-H --host -p --port -s -- secure -u --user --passwordfile

-I --interactive

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

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

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 is 4848.

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

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.

The --passwordfile option specifies the name, including the full path, 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.

administration server password, use an entry with the following format:

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.

For example, to specify the domain

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

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

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--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.

update-file-user.

--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.

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 valid only in domains that are configured to support clusters, such as domains

--uniquetablenames

--libraries

--target

Operands dirpath

that are created with the cluster profile or the enterprise profile. 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.

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.

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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.

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

error in executing the command

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

1

Name deploy-jbi-service-assembly – deploys a service assembly into the JBI environment

Synopsis deploy-jbi-service-assembly

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host]

[--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

[--enabled =true]

[--upload=true] [--target target] filepath or service_assembly_name

Description The deploy-jbi-service-assembly command deploys a service assembly into the JBI environment.

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 is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

administration server.

The authorized domain administration server -u --user

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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

If this option is set to true, the service assembly is started automatically when the system starts up. Users are allowed to access the service assembly. If this option is set to false, the service assembly is not started automatically when the system starts up. Users are not able to access the service assembly. For EE, this option enables the deployment on the specified target instance or cluster. This option is ignored when the service assembly is being deployed on the target domain.

When this option is set to true, the command uploads the file to the administration server. The file is uploaded to the \$JBI_HOME/tmp directory on the Domain Administration Server (DAS), for example,

--help

--enabled

--upload

--target

\$AS_INSTALL_DIR/domains/domain_name/jbi/tmp. If the filepath of the installable file is mounted to the server machine, or if the administration server is running locally, set the upload option to false.

Specifies the target on which you are deploying the service assembly. Specify this option only if the service assembly is deployed in a multiserver environment with a DAS. If the service assembly is not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which deploys the JBI service assembly on the embedded DAS instance. This is the default value.
- domain, which deploys the JBI service assembly for the administrative domain itself. Specify domain only if you are using the cluster profile.
- cluster_name, which deploys the JBI service assembly on every server instance in the cluster.
- instance_name, which deploys the JBI service assembly for the named unclustered server instance.

Operands *filepath or service_assembly_name*

The path to the archive file that contains the attributes of the JBI service assembly or the name of the service assembly that has been previously deployed to the domain.

Examples EXAMPLE 1 Using the deploy-jbi-service-assembly command

The following command deploys a JBI service assembly.

asadmin> deploy-jbi-service-assembly --user admin2
--passwordfile passwords.txt --target server1 filepath
Command deploy-jbi-service-assembly executed successfully.

Exit Status 0

command executed successfully

1

error in executing the command

See Also list-jbi-service-assemblies(1), show-jbi-service-assembly(1)

Name disable – disables the component

Synopsis disable

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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.

	have been deployed. If the component has not been deployed, an error message is returned		
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.	
	-Iinteractive	If set to true (default), only the required password options are prompted.	
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.	
	-pport	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 is 4848.	
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.	
	-uuser	The authorized domain administration server administrative username.	
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.	
	passwordfile	Thepasswordfile option specifies the name, including the full path, of a file containing the password entries in a	

uppercase letters.

specific format. The entry for the password must have the AS_ADMIN_ prefix followed by the password name in

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

name of the component to be disabled.

--help

--target

Operands component_name

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

Synopsis disable-http-lb-application

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
 [ --timeout 30]
 -- name application_name target
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide

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

> Once the application is disabled and the changes have been applied to the load balancer, new requests for the application are not forwarded to the target. Existing sessions continue to access the application until the timeout is reached. This process is known as quiescing.

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

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

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.

-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.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--help Displays the help text for the command.

--timeout (in minutes) to wait before disabling the

specified application. This time allows for the graceful shutdown (quiescing) of the specified application. The default value is 30 minutes. The minimum value is 1 minute.

--name The name of the application to be disabled.

Operands *target* This operand specifies the server instance or cluster on which to disable the application. Valid values are:

 cluster_name, which disables the application on all server instances in the cluster.

 stand-alone_instance_name, which disables the application on the stand-alone server instance.

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

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

Exit Status 0 command executed successfully

1 error in executing the command

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

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

Synopsis disable-http-lb-server

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --timeout 30]
target
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> This command disables a stand-alone server or cluster of servers for load balancing. The disabled server instance or cluster goes offline for load balancing with a minimum impact to users.

Once the target has been disabled and the changes have been applied to the load balancer, the load balancer stops assigning new requests to the target. Session requests with sessions created before disabling the target continue to be assigned to that target until the timeout is reached. This process is known as quiescing.

Apply changes to the load balancer either automatically, or using the command apply-http-lb-changes. You can also manually export the configuration using export-http-lb-config and copy it to the load balancer.

		1,
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.

-s --secure

-u --user

--passwordfile

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

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--help Displays the help text for the command.

--timeout (in minutes) to wait before disabling the

specified target. This time allows for the graceful shutdown (quiescing) of the specified target. The default value is 30

minutes. The minimum value is 1 minute.

Operands target This operand specifies which server instances and clusters to

disable. Valid values are:

 cluster_name, which disables all the server instances in the cluster.

 instance_name, which disables a standalone or clustered server instance.

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

 $\verb|asadmin>| \textbf{disable-http-lb-server}| \textbf{ --user}| \textbf{ admin}| \textbf{ --passwordfile}| \textbf{ filename}| \textbf{ mycluster}|$

Command disable-http-lb-server executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

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

Name display-error-distribution – displays distribution of errors from instance server.log at module

Synopsis display-error-distribution

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]
[--passwordfile filename] [--help]
[--target instance] timestamp

Description Displays distribution of errors from instance server. log at module level.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This is the name of the target upon which the command is operating. The valid targets for this command is instance.

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

--help

Operands --timestamp

--target

Before using display-error-distribution command, use the display-error-statistics command to get the timestamp, which is a required operand for the display-error-distribution command.

. .

	EXAMPLE 1 Using display-error-distrib	ribution (Continued)	
	asadmin> display-error-statisti Timestamp	Severity Warning	
	1185340505312(Jul 25, 2007 10:4	:45:05 AM) 0 0	
	1185336905312(Jul 25, 2007 9:45	45:05 AM) 0 0	
	1185333305312(Jul 25, 2007 8:45	45:05 AM) 0 0	
	1185329705312(Jul 25, 2007 7:45	45:05 AM) 0 0	
	1185326105312(Jul 25, 2007 6:45	45:05 AM) 0 0	
	Severity Warning moduleID 1 2 javax.ente	•	115

	Command display-error-distribut	ition 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

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]
[--target instancename/clustername]

Description This command displays a summary of list of severities and warnings in server. log since last server restart. This command can run both locally and remotely.

	server restart. This command can run both locally and remotery.	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	The HTTP/S port for administration. This is the port to

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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This is the name of the target upon which the command is operating. The valid targets for this command are instance and cluster.

--help

--target

Examples EXAMPLE 1 Using display-error-statistics

asadmin> display-error-statistics

Timestamp	Severity	Warning
1185340505312(Jul 25, 2007 10:45:05 AM)	1	20
1185336905312(Jul 25, 2007 9:45:05 AM)	0	0
1185333305312(Jul 25, 2007 8:45:05 AM)	0	0
1185329705312(Jul 25, 2007 7:45:05 AM)	0	0
1185326105312(Jul 25, 2007 6:45:05 AM)	0	0

EXAMPLE 1 Using display-error-statistics (Continued)

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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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. -T -- 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. The HTTP/S port for administration. This is the port to -p --port which you should point your browser in order to manage the domain. For example, http://localhost:4848. The default port number is 4848. If set to true, uses SSL/TLS to communicate with the domain -s --secure administration server. The authorized domain administration server -u --user 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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

Examples EXAMPLE 1 Using display-license in local mode

asadmin> displav-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

EXAMPLE 2 Using display-license in remote mode (Continued)

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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile *filename*] [--help] --errorlevel {SEVERE|WARNING} --timestamp [--target instance] {module-id [modul **Description** This command displays all the error messages for a given module at a given timestamp. This command can run 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. Setting to true will echo the command line statement on the -e --echo standard output. Default is false. -I --interactive If set to true (default), only the required password options are prompted. The machine name where the domain administration server -H --host is running. The default value is localhost. The HTTP/S port for administration. This is the port to -p --port which you should point your browser in order to manage the domain. For example, http://localhost:4848. The default port number is 4848. If set to true, uses SSL/TLS to communicate with the domain -s --secure 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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--help Displays the help text for the command.

--target This is the name of the target upon which the command is operating. The valid targets for this command are instance

and cluster.

--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

Before using the display-log-records command, use the display-error-statistics and the display-error-distribution command to get the timestamp and module id, which are required operands for the display-log-records command.

EXAMPLE 1 Using display-log-records (Continued)

```
asadmin> display-error-statistics
Timestamp
                                   Severity Warning
-----
1185340505312(Jul 25, 2007 10:45:05 AM)
                                      1
                                              20
1185336905312(Jul 25, 2007 9:45:05 AM)
1185333305312(Jul 25, 2007 8:45:05 AM)
                                       a
                                              a
1185329705312(Jul 25, 2007 7:45:05 AM)
                                       0
                                               0
1185326105312(Jul 25, 2007 6:45:05 AM)
......
Command display-error-statistics executed successfully.
asadmin> display-error-distribution 1185340505312
************************
Severity Warning moduleID
        2
                 javax.enterprise.system.container.web
0
         18
               javax.enterprise.system.tools.admin.server.mbeans
*************************
Command display-error-distribution executed successfully.
asadmin> display-log-records --passwordfile
passwords --user admin --target server --host localhost --timestamp 1185340505312
--port 4848 javax.enterprise.system.container.web
RecNumber = 5849
dateTime = Wed Jul 25 10:45:05 AM PST 2007
msqId = WEB0335
level = WARNING
productName = sun-appserver-9.1
logger = javax.enterprise.system.container.web
nvp = ThreadID=10; ThreadName=main; RequestID=a4a52e69-ed14-4d0c-ada7-4fe07382c158;
message = http-listener attribute family not supported
RecNumber = 5848
dateTime = Wed Jul 25 10:45:05 AM PST 2007
msqId = WEB0334
level = WARNING
productName = sun-appserver-9.1
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.
```

Name enable – enables the component

Synopsis enable

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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

	mode only.	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.

The -- passwordfile option specifies the name, including the full path, of a file containing the password entries in a

--passwordfile

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

--target

instance_name, which enables a particular server instance

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 enable-http-lb-application – enables a previously-disabled application managed by a load balancer

```
Synopsis enable-http-lb-application
          [--terse={true|false}][ --echo={true|false} ]
          [ --interactive={true|false} ] [ --host host]
          [--port port] [--secure| -s ] [ --user admin_user]
          [--passwordfile filename] [--help]
            -- name application_name
           target
```

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> When applications are deployed, by default they are disabled for load balancing. Use this command to enable applications deployed on a stand-alone instance or cluster for load balancing. Enable the application on all instances in a cluster, or on a single standalone server instance.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The name of the application to be enabled.

This operand specifies on which server instance or cluster to enable the application. Valid values are:

--help

--name

Operands target

- *cluster_name*, which enables the application on all server instances in the cluster.
- stand-alone_instance_name, which enables the application in the stand-alone server instance.

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

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

Exit Status 0 command executed successfully

1 error in executing the command

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

Name enable-http-lb-server – enables a previously disabled sever or cluster managed by a load balancer

Synopsis enable-http-lb-server

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
target
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> This command enables a stand-alone server instance or cluster for load balancing. By default, load balancing is disabled for instances and clusters.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser

option on subsequent operations to this particular domain.

--passwordfile

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This operand specifies which server instances and clusters to enable. Valid values are:

- cluster_name, which enables all the server instances in the cluster.
- instance_name, which enables a standalone or clustered server instance.

--help

Operands target

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

asadmin> enable-http-lb-server --user admin --passwordfile filename mycluster Command enable-http-lb-server executed successfully.

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

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

Name export – marks a variable name for automatic export to the environment of subsequent commands in multimode

Synopsis export [name=value [name=value]*]

Description 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 as admin. 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 export-http-lb-config – exports the load balancer configuration or load balancer to a file

Synopsis export-htp-lb-config

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
 --config config name | --lbname load balancer name [--retrieve=false] [file name]
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> Use the export-http-lb-config command to export a load balancer configuration or load balancer into a file that the load balancer plug-in can use. The default file name is loadbalancer.xml, but you can specify a different name. Once exported, you manually copy the exported file to the load balancer plug-in location before configuration changes are applied.

> To apply changes to the load balancer without manually copying the configuration file, use apply-http-lb-changes, or configure the load balancer to automatically apply changes with create-http-lb. If you use these commands, you do not need to use export-http-lb-config.

Options	-tterse	
Options		

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring

well-formatted data for consumption by a script. Default is

false.

-e --echo Setting to true will echo the command line statement on the

standard output. Default is false.

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

are prompted.

The machine name where the domain administration server -H --host

is running. The default value is localhost.

The HTTP/S port for administration. This is the port to -p --port

which you should point your browser in order to manage the

domain. For example, http://localhost:4848.

The default port number is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

administration server.

-u --user

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies which load balancer configuration to export.

--help

--config

--1hname

--retrieve

Operands file name

balancer. Specifying both results in an error.

Specifies the load balancer to export.

Specify either a load balancer configuration or a load balancer. Specifying both results in an error.

Specify either a load balancer configuration or a load

If set to true, retrieves the loadbalancer.xml file from the remote machine. The default is false.

Specifies the file name and location of the exported configuration.

- If you specify a directory (relative or absolute) but not a
 file name, the file named
 loadbalancer.xml.load_balancer_config_name is
 created in the specified directory. On Microsoft
 Windows systems the path must be in quotes.
- If you specify a file name in a relative or absolute path, the file is created with the name you specify in the directory you specify.
- If you specify a file name but do not specify a directory, the file is created with that name in the current working directory.
- If you do not specify this operand, the default value is a file named loadbalancer.xml.load_balancer_config_name created in the app_sever_install/domains/domain_name/generated directory.

Examples EXAMPLE 1 Using the export-http-lb-config command on the UNIX platform

The following example exports the load balancing configuration mycluster-http-lb-config to a file named loadbalancer.xml in the /Sun/AppServer directory.

asadmin> export-http-lb-config --user admin --passwordfile file --config mycluster-http-lb-config /Sun/AppServer/loadbalancer.xml Command export-http-lb-config executed successfully.

EXAMPLE 2 Using the export-http-lb-config command on the Microsoft Windows platform

The following example exports the load balancing configuration mycluster-http-lb-config to a file named loadbalancer.xml in the C:\Sun\AppServer directory on a Microsoft Windows system.

asadmin> export-http-lb-config --user admin --passwordfile file
--config mycluster-http-lb-config "C:\Sun\AppServer\loadbalancer.xml"
Command export-http-lb-config executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

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

Name flush-jmsdest – purges messages in a JMS destination.

Synopsis flush-imsdest

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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 is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

administration server.

The authorized domain administration server -u --user

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, including

> the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

--target

This option is valid only in domains that are configured to support clusters, such as domains that are created with the

cluster profile or the enterprise profile.

---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 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), create-jmsdest(1)

Name freeze-transaction-service – freezes the transaction subsystem

Synopsis freeze-transaction-service

[--terse={true|false}][--echo={true|false}]

[--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help] [--target 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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help target **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 unfreeze-transaction-service(1), rollback-transaction(1)

Name generate-diagnostic-report – generates reports that can help diagnose application server malfunctioning

```
Synopsis generate-diagnostic-report
                                        --outputfile jar_file_name
          [--terse={true|false}][ --echo={true|false} ]
          [ --interactive={true|false} ] [ --host host]
          [--port port] [--secure| -s ] [ --user admin_user]
          [--passwordfile filename] [--help]
           [ --local =false] [--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	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.
	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.

-s --secure

-u --user

--passwordfile

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

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--help

--file

Displays the help text for the command.

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.

- instance: generates report for a particular server instance.
- nodeagent: generates reports for all server instances associated with a specific node agent.

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 domain1

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/software/sjsas/diagnostic-reports/domain1.jar
- --targetdir /export/software/sjsas/domains domain1

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 command 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-jym-report – shows the threads, classes and memory for a given target instance.

Synopsis generate-jvm-report

Options -t--terse

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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.

Indicates that any output data must be very concise, typically

the full path, of a file containing the password entries in a

avoiding human-friendly sentences and favoring

	well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
-Iinteractive	If set to true (default), only the required password options are prompted.
-Hhost	The machine name where the domain administration server is running. The default value is localhost.
-pport	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 is 4848.
-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
-uuser	The authorized domain administration server administrative username.
	If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
passwordfile	Thepasswordfile option specifies the name, including

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

--type

 threads, which provides information about threads running and the thread dump (stack trace) for a given target instance.

Operands target

1

This option specifies the ending location of the connector resources. Valid targets are server, domain, cluster, and instance. The default target is server.

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
```

error in executing the command

Name get – gets the values of the monitorable or configurable attributes

Synopsis get

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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.
- 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
	<pre>default-config.admin-service</pre>
	<pre>default-config.admin-service.das-config</pre>
	<pre>default-config.admin-service.jmx-connector.system</pre>
	<pre>default-config.admin-service.jmx-connector.system.ssl</pre>
	<pre>default-config.availability-service</pre>
	<pre>default-config.availability-service.jms-availability</pre>
	<pre>default-config.diagnostic-service</pre>
	<pre>default-config.ejb-container</pre>
	•
	<pre>default-config.http-service.http-listener.http-listener-1</pre>
	<pre>default-config.http-service.http-listener.http-listener-2</pre>
	•
	<pre>default-config.iiop-service</pre>
	•
	<pre>default-config.java-config</pre>
	•
	■ domain
	<pre>domain.clusters</pre>
	<pre>domain.configs</pre>
	<pre>domain.resources</pre>
	domain.resources.jdbc-connection-pool.DerbyPool
	domain.resources.jdbc-connection-poolCallFlowPool
	<pre>domain.resources.jdbc-connection-poolTimerPool</pre>
	•
	■ server
	■ server-config
	<pre>cerver-config.admin-service</pre>
	<pre>server-config.admin-service.das-config</pre>
	<pre>server-config.admin-service.jmx-connector.system</pre>
	<pre>server-config.admin-service.jmx-connector.system.ssl</pre>
	<pre>server-config-availability-servicce</pre>
	<pre>server-config.availability-service.jms-availability</pre>
	<pre>server-config.diagnostic-service</pre>
	<pre>server-config.ejb-container</pre>
	•
	■ server.log-service
	<pre>server.log-service.module-log-levels</pre>
	•
	<pre>server.session-config</pre>
	<pre>server.session-config.session-manager</pre>
	<pre>server.session-config.session-manager.manager-properties</pre>
	<pre>server.session-config.session-manager.store-properties</pre>
n Java System App	 server.session-config.session-properties lication Server 9.1 Reference Manual selection Server 1. Thread-pools
	<pre>server.thread-pools.thread-pool-1</pre>
	·

Command	Output	
list -monitor *	<pre>server server.applications server.applicationsJWSappclients server.applicationsJWSappclients.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 server.orb.connection-managers server.resources server.thread-pools</pre>	

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 thelist 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 thelist 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	 default-config.http-service. http-listener.http-listener-1 default-config.http-service. http-listener.http-listener-2 server-config.http-service. http-listener.admin-listener server-config.http-service. http-listener.http-listener-1 server-config.http-service. http-listener.http-listener-2 server-http-service.http-listener.admin-listener server.http-service.http-listener.http-listener-1 server.http-service.http-listener.http-listener-1
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.http-listener.ontext.	server.http-service.http-listener.http-listener-1.acceptor-threads = 1 server.http-service.http-listener.http-listener-1.address = 0.0.0.0 server.http-service.http-listener.http-listener-1.blocking-enabled = false server.http-service.http-listener.http-listener-1.default-virtual-se = server server.http-service.http-listener.http-listener-1.enabled = true server.http-service.http-listener.http-listener-1.external-port = server.http-service.http-listener.http-listener-1.family = inet server.http-service.http-listener.http-listener-1.id = http-listener-1 server.http-service.http-listener.http-listener-1.port = 8080 server.http-service.http-listener.http-listener-1.redirect-port = server.http-service.http-listener.http-listener-1.security-enabled = false server.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-service server.monitoring-service.module-monitoring-levels
		Note that this is the list command. It only shows the hierarchy, nothing else. Using the ' ' and "grep" narrows down the search effectively. Now, you can choose server.monitoring-service to set the attributes of various attributes that can be monitored.
		This is the configuration data because this setting will be persisted to the server's configuration store.
2	get server.monitoring-service.*	You can try the number of attributes that are presently available with monitoring service. Here is the output:
		No matches resulted from the wildcard expression. This is because this fully dotted name does not have any attributes at all. Logically, you try the next one and that is: server.monitoring-service.module-monitoring-levels. Again, use the wildcard character to get ALL the attributes of a particular component.

ID	Command	Output/Comment
3	get server.monitoring-service. module-monitoring-levels.*	server.monitoring-service.module-monitoring-levels. connector-connection-pool = 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-pool = 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. transaction-service = 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.	$server.monitoring-service.module-monitoring-levels.jvm \\ = HIGH$
	j vm=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	listmonitor * 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-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.dotted-name =
	server.jvm.class-loading-	server.jvm.class-loading-system
	system.*	server.jvm.class-loading-system.loadedclasscount-count = 7328
		server.jvm.class-loading-system.loadedclasscount-description = No Description was available
		$server.jvm.class-loading-system.loaded class count-last sample time \\ = 1133819508973$
		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-lastsamplet = 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-lastsampletin = 1133819508973
		server.jvm.class-loading-system.unloadedclasscount-name = UnloadedClassCount?
		server.jvm.class-loading-system.unloadedclasscount-starttime = 1133819131268
		$server.jvm.class-loading-system.unloaded class count-unit\\=count$
		You can see 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.

-Hhost	The machine name where the domain administration server is running. The default value is localhost.
-pport	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 is 4848.
-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
-uuser	The authorized domain administration server administrative username.
	If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
passwordfile	Thepasswordfile option specifies the name, including the full path, 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 throughpasswordfile 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 thepasswordfile or enter them at the command prompt.

Setting to true will echo the command line statement on the

If set to true (default), only the required password options

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin

standard output. Default is false.

are prompted.

-e--echo

-I --interactive

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

defaults to false; if set to false, the configurable attribute values are returned. If set to true, the monitorable attribute values are returned.

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>

--monitor

--help

Operands attributename

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*.*.

EXAMPLE 1 Using the get command with wildcard (Continued)

Command	Operation
<pre>get *config*.*.*</pre>	gets all values on the dotted names which match "*config*.*"
get domain.j2ee-applications.*.ejb-module.*.*	gets all values on all ejb-modules of all applications.
get *web-modules.*.*	get all values on all web modules whether in an application or standalone.
get *.*.*.*	get all values on all dotted names which have three parts.

EXAMPLE 2 Using get with the monitor option

To get the monitoring data from the domain administration server, the appropriate monitoring level must be set on the appropriate subsystem. Use the set command to set the monitoring data level. For example, to set the monitoring level on Web Container on Domain Administration Server (DAS) to HIGH so that the Web Container returns many monitorable attributes and their values:

server.monitoring-service.module-monitoring-levels.web-container=HIGH. See the set command for further details on setting the monitoring level.

Top Level

Command	Dotted Name	Output
get -m		No output, but message saying there are no attributes at this node.

Applications Level

Command	Dotted Name	Output
get -m	server.applications.* or *applications.*	No output, but message saying there are no attributes at this node.

Applications — Enterprise Applications and Standalone Modules

Command	Dotted Name	Output
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.

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	List of Attributes and Values corresponding to attributes as defined under EJBPoolStats Statistics.
	Note: Where it is a standalone module, the node app1 will not appear.	

Command	d Dotted Name Output	
get -m	server.applications.app1.ejb- module1_jar.bean1.bean-cache.* Note: Where it is a standalone module, the node app1 will not appear.	List of Attributes and Values corresponding to attributes as defined under EJBCacheStats Statistics.
get -m	server.applications.app1. ejb-module1_jar.bean1.bean- cachemethod.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

Command	Dotted Name	Output
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

Command	Dotted Name	Output
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

Command	Dotted Name	Output
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

	Command	Dotted Name	Output
ge	et -m		List of Attributes and Values corresponding to JTAStats Statistics.

ORB Level

Command	Dotted Name	Output
get -m	server.orb.*	No output, but message saying there are no attributes at this node.
get -m	server.orb.connection-managers.*	No output, but message saying there are no attributes at this node.
get -m	server.orb.connection-managers. orbconnmgr1.*	Attributes and values corresponding to OrbConnectionManagerStats Statistics.

JVM Level

Command	Dotted Name	Output
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 High
		WaterMark = 45490176
		server.jvm.HeapSize Last
		SampleTime = 1063217002433
		server.jvm.HeapSize LowWaterMark = 0
		server.jvm.HeapSize LowerBound = 0
		server.jvm.HeapSize Name = JvmHeapSize
		server.jvm.HeapSize_StartTime =
		1063238840055
		server.jvm.HeapSize_Unit = bytes
		server.jvm.HeapSize_
		UpperBound = 531628032
		server.jvm.UpTime_Count = 1063238840100
		server.jvm.UpTime_Description =
		Describes JvmUpTime
		server.jvm.UpTime_LastSampleTime =
		1-63238840070
		server.jvm.UpTime_Name = JvmUpTime
		server.jvm.UpTime_StartTime = 1063217002430
		server.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 --appname application_name [--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help]

[--target target_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	appname	name of the application.
	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser

option on subsequent operations to this particular domain.

The -- passwordfile option specifies the name, including the full path, of a file containing the password entries in a

--passwordfile

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

path to the local directory where the client stub should be stored.

Examples EXAMPLE 1 Using get-client-stubs

--help

Operands *local_directory_path*

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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 Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

-t --terse

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.

-e --echo

Setting to true will echo the 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 is 4848.

-s --secure

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

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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

- -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 ()

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 man page 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
             apply-http-lb-changes
                applies load balancer configuration changes to the load balancer
             backup-domain
                performs a backup on the domain
             change-admin-password
                changes the administrator password
             change-master-password
                changes the master password
             clear-ha-store
                deletes tables in the HA database
             configure-ha-cluster
                configures an existing cluster to be High Availability
             configure-ha-persistence
                enables configuration of parameters related to session persistence
             configure-lb-weight
                sets load balancing weights for clustered instances
             configure-webservice-management
                sets the monitoring or maxhistory or attributes of a deployed webservice
             copy-config
                copies an existing configuration to create a new configuration
             create-admin-object
                adds the administered object with the specified JNDI name
             create-application-ref
                creates a reference to an application
```

```
create-audit-module
  creates an audit module for the optional plugin module
create-auth-realm
  adds the named authorized realm
create-cluster
  creates a cluster
create-connector-connection-pool
  adds a connection pool with the specified connection pool name
create-connector-resource
  registers the resource with the specified JNDI name
create-connector-security-map
  creates or modifies a security map for the 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-ha-store
  creates tables in HA database that are used by HA cluster
create-http-health-checker
  creates a health-checker for a specified load balancer configuration
create-http-lb
  creates a load balancer
create-http-lb-config
  creates a configuration for the load balancer
create-http-lb-ref
  add an existing cluster or server instance to an existing load balancer configuration
create-http-listener
  adds a new HTTP listener socket
create-iiop-listener
  adds the IIOP listener
create-instance
  creates an instance with the given name
create-javamail-resource
  registers the Javamail resource
```

```
create-jdbc-connection-pool
   registers the JDBC connection pool
create-jdbc-resource
   registers the JDBC resource
create-jms-host
   creates a IMS host
create-jms-resource
  registers the JMS resource
create-jmsdest
  adds the named destination
create-indi-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-node-agent-config
   adds a new unbound node agent to a domain
create-node-agent
   creates a node agent and its associated directory structure
create-password-alias
   creates a password alias
create-persistence-resource
   registers the persistence resource
create-profiler
  creates the profiler element
create-resource-adapter-config
  creates the resource adapter Java bean
```

```
create-resource-ref
   creates a reference to a resource
create-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-system-properties
   adds or updates one or more system properties of the domain, configuration, cluster, or
   server instance
create-threadpool
   creates the thread pool
create-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-application-ref
   removes a reference to an application
delete-audit-module
   deletes the audit-module for the optional plugin module
delete-auth-realm
   removes the named authorized realm
delete-cluster
   deletes a cluster
delete-config
   deletes an existing configuration
delete-connector-connection-pool
   removes the specified connection pool
delete-connector-resource
   removes the named resource connector
delete-connector-security-map
   deletes the named security map
delete-custom-resource
   removes the custom resource
```

```
delete-domain
  deletes the given domain
delete-file-user
   removes the named file user
delete-http-health-checker
  deletes a health-checker for a specified load balancer configuration
delete-http-lb
   deletes a load balancer
delete-http-lb-config
   deletes a load balancer configuration
delete-http-lb-ref
   deletes the cluster or server instance from a load balancer configuration
delete-http-listener
  removes the HTTP listener
delete-iiop-listener
  removes the IIOP listener
delete-instance
   deletes the instance that is not running
delete-javamail-resource
   removes the Javamail resource
delete-jdbc-connection-pool
  removes the JDBC connection pool
delete-jdbc-resource
   removes the JDBC resource
delete-jms-host
  removes a JMS host
delete-jms-resource
  removes the IMS 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-node-agent-config
  removes a node agent from a domain
delete-node-agent
  deletes the node agent and its associated directory structure
delete-password-alias
  deletes a password alias
delete-persistence-resource
  removes the persistence resource
delete-profiler
  deletes the profiler element
delete-resource-adapter-config
  deletes the resource adapter Java bean
delete-resource-ref
  removes a reference to a resource
delete-ssl
  deletes the ssl element from the HTTP listener or IIOP listener
delete-system-property
  removes one or more system properties of the domain, configuration, cluster, or server
  instance
delete-threadpool
  deletes the thread pool
delete-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-jbi-service-assembly
  deploys a service assembly into the JBI environment
deploy
  deploys the specified component
```

```
deploydir
   deploys the component that is in the specified directory, located in the domain application
   server
disable-http-lb-server
   disables a sever or cluster managed by a load balancer
disable-http-lb-application
   disables an application managed by a load balancer
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-http-lb-application
   enables a previously-disabled application managed by a load balancer
enable-http-lb-server
   enables a previously disabled sever or cluster managed by a load balancer
enable
  runs the specified, deployed component
export-http-lb-config
   exports the load balancer configuration to a file that can be used by the load balancer
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
get-health
   provides information on the cluster health
help
   displays a list of all the commands available in the command-line interface
install-jbi-component
   installs a service engine or binding component into the JBI environment
install-jbi-shared-library
   installs a shared library into the JBI environment
jms-ping
   checks to see if the JMS provider is running
list-admin-objects
   lists all the administered objects
list-application-refs
   lists all application references in a cluster or unclustered server instance
list-audit-modules
   lists the audit modules
list-auth-realms
   lists the authorized realms
list-backups
   lists all backups and restores
list-clusters
   lists the existing clusters
list-components
   lists deployed components
list-configs
   lists all existing configurations
list-connector-connection-pools
   gets all the connection pools
list-connector-resources
   gets all the connector resources
list-connector-security-maps
   lists the security maps for the connector connection pool
list-custom-resources
   gets all the custom resources
```

lists the domains in the given domains directory

list-file-groups lists the file groups

list-file-users lists the file users

list-http-lb-configs lists load balancer configurations

list-http-lbs lists load balancers

list-http-listeners gets the HTTP listeners

list-iiop-listeners gets the IIOP listeners

list-instances lists all the instances in the server

list-javamail-resources gets all the Javamail resources

list-jdbc-connection-pools registers the JDBC connection pool

list-jdbc-resources gets all the JDBC resources

list-jbi-binding-components lists the binding components installed on the specified target

list-jbi-service-assemblies lists the service assemblies installed into the JBI environment

list-jbi-service-engines lists the service engines installed on the specified target

list-jbi-shared-libraries lists the JBI shared libraries that are installed into the JBI environment

list-jms-hosts lists the existing JMS hosts

list-jms-resources gets all the JMS resources

list-jmsdest gets all the named destinations list-jndi-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-node-agents lists the node agents along with their status list-password-aliases lists all password aliases list-persistence-resources gets all the persistence resources list-registry-locations returns list of configured web service registry access points list-resource-adapter-configs lists the resource adapters configured in an instance list-resource-refs lists the existing resource references list-sub-components lists EJBs or Servlets in a deployed module or in a module of a deployed application list-system-properties lists the system properties of the domain, configuration, cluster, or server instance list-threadpools lists the thread pools list-timers lists all of the timers owned by server instance(s) list-transformation-rules lists all the transformation rules of a given webservice

gets all the named destinations, browses and queries the JNDI tree

list-indi-entries

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
login
  lets you log in to a domain
migrate-timers
  moves a timer when a server instance stops
monitor
  displays monitoring data for commonly-used Application Server components
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
remove-ha-cluster
   returns an HA cluster to non-HA status
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
show-jbi-binding-component
   shows detailed information about the specified binding component
show-jbi-service-assembly
   shows detailed information about a specified service assembly
show-jbi-service-engine
   shows detailed information about the specified service engine
```

```
show-jbi-shared-library
  shows detailed information about a specified shared library
shut-down-jbi-component
  shuts down a service engine or a binding component on the specified target
shut-down-jbi-service-assembly
  shuts down a JBI service assembly on the specified target
start-appserv
  starts the domains in the specified domains directory
start-callflow-monitoring
  provides the complete callflow/path of a request
start-cluster
  starts a cluster
start-database
  starts the bundled Java DB database
start-domain
  starts the given domain
start-instance
  starts a server instance
start-jbi-component
  starts a service engine or a binding component on the specified target
start-jbi-service-assembly
  starts a service assembly on the specified target
start-node-agent
  starts a node agent
stop-appserv
  stops the domains in the specified domains directory
stop-callflow-monitoring
  disables collection of callflow information of a request
stop-cluster
  stops a cluster
stop-database
  stops the bundled Java DB database
stop-domain
  stops the given domain
stop-instance
  stops a server instance
```

```
stop-jbi-component
   stops a service engine or a binding component on the specified target
stop-jbi-service-assembly
   stops a service assembly on the specified target
stop-node-agent
  stops a node agent
undeploy-jbi-service-assembly
   undeploys a service assembly on the specified target
undeploy
   removes a component in the domain application server
unfreeze-transaction-service
   mobilizes the named transaction service
uninstall-jbi-component
  uninstalls a service engine or binding component on the specified target
uninstall-jbi-shared-library
   uninstalls a shared library on the specified target
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
The following commands are deprecated:
■ display-license
  install-license
```

- restart-instance
- shutdown
- create-acl

- delete-acl
- list-acls
- start-appserv
- stop-appserv

Examples Example 1 Using help

asadmin> help

asadmin> create-domain --help

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

See Also asadmin(1M)

Name install-jbi-component – installs a service engine or binding component into the JBI environment

Synopsis install-jbi-component

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [--enabled =true] [--properties : [(name=value) [:name=value]... | file]] [--upload=true] [--target target] filepath or component_name

Description The install-jbi-component command installs a service engine or binding component into the JBI environment.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

If this option is set to true, the component is started automatically when the system starts up. Users are allowed to access the component. If this option is set to false, the component is not started automatically when the system starts up. Users are not able to access the component. For EE, this option enables the component on the specified target instance or cluster. This option is ignored when the component is being deployed on the target domain.

--help

--enabled

---properties

Property values that are to be set for the component. The option can be specified as a string of keyword-value pairs, or the name of a property file can be provided.

--upload

When this option is set to true, the command uploads the file to the administration server. The file is uploaded to the \$JBI_HOME/tmp directory on the Domain Administration Server (DAS), for example,

\$AS_INSTALL_DIR/domains/domain_name/jbi/tmp. If the filepath of the installable file is mounted to the server machine, or if the administration server is running locally, set this option to false.

--target

Specifies the target on which you are installing the JBI component. Specify this option only if you are installing the JBI component in a multiserver environment with a DAS. If you are not installing the JBI component in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which installs the JBI component on the embedded DAS instance. This is the default value.
- domain, which installs the JBI component on the administrative domain itself. Specify domain only if you are using the cluster profile.
- cluster_name, which installs the JBI component on every server instance in the cluster.
- instance_name, which installs the JBI component on the named unclustered server instance.

Operands *filepath or component_name*

The path to the archive file that contains the attributes of the JBI component or the name of the JBI component or service assembly that has previously been installed.

Examples EXAMPLE 1 Using the install-jbi-component command

The following command installs a JBI component.

```
asadmin> install-jbi-component --user admin2
--passwordfile passwords.txt --target server1 filepath
Command install-jbi-component executed successfully.
```

Exit Status 0

command executed successfully

1 error in executing the command

See Also start-jbi-component(1), list-jbi-binding-components(1), list-jbi-service-engines(1), stop-jbi-component(1), shut-down-jbi-component(1), uninstall-jbi-component(1)

Name install-jbi-shared-library – installs a shared library into the JBI environment **Synopsis** install-jbi-shared-library [--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [--upload =true] [--target target] filepath or shared_library_name **Description** The install-jbi-shared-library command installs a shared library into the JBI environment. 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 Setting to true will echo the command line statement on the -e --echo standard output. Default is false. -I --interactive If set to true (default), only the required password options are prompted. The machine name where the domain administration server -H --host is running. The default value is localhost. The HTTP/S port for administration. This is the port to -p --port which you should point your browser in order to manage the domain. For example, http://localhost:4848. The default port number is 4848. If set to true, uses SSL/TLS to communicate with the domain -s --secure 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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

When this option is set to true, the command uploads the file to the administration server. The file is uploaded to the \$JBI_HOME/tmp directory on the Domain Administration Server (DAS), for example,

\$AS_INSTALL_DIR/domains/domain_name/jbi/tmp. If the filepath of the installable file is mounted to the server machine, or if the administration server is running locally, set the upload option to false.

Specifies the target on which you are installing the JBI shared library. Specify this option only if you are installing the JBI shared library in a multiserver environment with a DAS. If

--help

--upload

--target

you are not installing the JBI shared library in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which installs the JBI shared library on the embedded DAS instance. This is the default value.
- domain, which installs the JBI shared library on the administrative domain itself. Specify domain only if you are using the cluster profile.
- cluster_name, which installs the JBI shared library on every server instance in the cluster.
- instance name, which installs the IBI shared library on the named unclustered server instance.

Operands *filepath or shared_library_name*

The path to the archive file that contains the JBI shared library or the name of a JBI shared library that has previously been installed into a domain.

Examples EXAMPLE 1 Using the install-jbi-shared-library command

The following command installs a JBI shared library.

asadmin> install-jbi-shared-library --user admin2 --passwordfile passwords.txt --target server1 filepath Command install-jbi-shared-library executed successfully.

Exit Status 0

command executed successfully

1

error in executing the command

See Also list-jbi-shared-libraries(1), show-jbi-shared-library(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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

Operands target

instance_name, which pings the JMS service for a particular server instance

This operand is valid in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

Examples EXAMPLE 1 Using the jms-ping command

The following command checks to see if the JMS service is running on the server instance server1:

```
asadmin> jms-ping --user admin
--passwordfile passwords.txt --host bluestar --port 4848
server1

JMS Ping Status=RUNNING
Command jms-ping executed successfully.
```

Exit Status 0

command executed successfully

l error in executing the command

See Also create-jmsdest(1), create-jms-resource(1)

Name list – lists the configurable elements

Synopsis list

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --monitor = 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.
- 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		
	<pre>default-config.admin-service</pre>		
	default-config.admin-service.das-config		
	<pre>default-config.admin-service.jmx-connector.system</pre>		
	<pre>default-config.admin-service.jmx-connector.system.ssl</pre>		
	<pre>default-config.availability-service</pre>		
	default-config.availability-service.jms-availability		
	<pre>default-config.diagnostic-service</pre>		
	<pre>default-config.ejb-container</pre>		
	■ Land		
	default-config.http-service.http-listener.http-listener-1		
	<pre>default-config.http-service.http-listener.http-listener-2</pre>		
	•		
	<pre>default-config.iiop-service</pre>		
	•		
	default-config.java-config		
	· · · · ·		
	■ domain		
	domain.clusters		
	<pre>domain.configs</pre>		
	<pre>domain.resources</pre>		
	domain.resources.jdbc-connection-pool.DerbyPool		
	domain.resources.jdbc-connection-poolCallFlowPool		
	domain.resources.jdbc-connection-poolTimerPool		
	■ Land		
	■ server		
	<pre>server-config</pre>		
	<pre>cerver-config.admin-service</pre>		
	<pre>server-config.admin-service.das-config</pre>		
	<pre>server-config.admin-service.jmx-connector.system</pre>		
	server-config.admin-service.jmx-connector.system.ssl		
	server-config-availability-servicce		
	server-config.availability-service.jms-availability		
	<pre>server-config.diagnostic-service</pre>		
	<pre>server-config.ejb-container</pre>		
	•		
	<pre>server.log-service</pre>		
	<pre>server.log-service.module-log-levels</pre>		
	•		
	<pre>server.session-config</pre>		
	<pre>server.session-config.session-manager</pre>		
	<pre>server.session-config.session-manager.manager-properties</pre>		
	<pre>server.session-config.session-manager.store-properties</pre>		
	server.session-config.session-properties Section 1: Administration Commands Section 1: Administration Commonds	2	

server.thread-pools.thread-pool.thread-pool-1

■ server.transaction-service

Command	Output
Command list -monitor *	Output server server.applications server.applicationsJWSappclients server.applicationsJWSappclients.sys\.war server.applications.adminapp server.applications.admingui server.connector-service server.http-service server.http-service.server server.jms-service server.jym
	server.orbserver.orb.connection-managersserver.resources
	<pre>server.thread-pools</pre>

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 thelist 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	 default-config.http-service. http-listener.http-listener-1 default-config.http-service. http-listener.http-listener-2 server-config.http-service. http-listener.admin-listener server-config.http-service. http-listener.http-listener-1 server-config.http-service. http-listener.http-listener-2 server-thtp-service.http-listener.admin-listener server.http-service.http-listener.http-listener-1 server.http-service.http-listener.http-listener-2
2	To find the listener that corresponds to the default http-listener where the web applications in the domain/server are deployed: 1. Examine the dotted name starting with item number 7 in above output. 2. Use the get command as shown in its usage. For example, get server. http-service.http-listener-1.* will return all the attributes of the http-listener in context.	server.http-service.http-listener.http-listener-1.acceptor-threads = 1 server.http-service.http-listener.http-listener-1.address = 0.0.0.0 server.http-service.http-listener.http-listener-1.blocking-enabled = false server.http-service.http-listener.http-listener-1.default-virtual-server-new = server server.http-service.http-listener.http-listener-1.enabled = true server.http-service.http-listener.http-listener-1.external-port = server.http-service.http-listener.http-listener-1.family = inet server.http-service.http-listener.http-listener-1.id = http-listener-1 server.http-service.http-listener.http-listener-1.port = 8080 server.http-service.http-listener.http-listener-1.redirect-port = server.http-service.http-listener.http-listener-1.security-enabled = false server.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	l list server* grep monitoring	server-config.monitoring-service server-config.monitoring-service.module-monitoring-levels server.monitoring-service server.monitoring-service.module-monitoring-levels
		Note that this is the list command. It only shows the hierarchy, nothing else. Using the ' ' and "grep" narrows down the search effectively. Now, you can choose server.monitoring-service to set the attributes of various attributes that can be monitored.
		This is the configuration data because this setting will be persisted to the server's configuration store.
2	get server.monitoring-service.*	You can try the number of attributes that are presently available with monitoring service. Here is the output:
		No matches resulted from the wildcard expression. This is because this fully dotted name does not have any attributes at all. Logically, you try the next one and that is: server.monitoring-service.module-monitoring-levels. Again, use the wildcard character to get ALL the attributes of a particular component.

ID	Command	Output/Comment
3	get server.monitoring-service. module-monitoring-levels.*	server.monitoring-service.module-monitoring-levels. connector-connection-pool = 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-pool = 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. transaction-service = 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	<pre>set server.monitoring-service. module-monitoring-levels. jvm=HIGH There is no space before or after the = sign.</pre>	$server.monitoring-service.module-monitoring-levels.jvm \\ = HIGH$
		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	listmonitor * grep 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-793827
		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.dotted-name =
	server.jvm.class-loading-	server.jvm.class-loading-system
	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-lastsampletin = 1133819508973
		<pre>server.jvm.class-loading-system.loadedclasscount-name = LoadedClassCount?</pre>
		server.jvm.class-loading-system.loadedclasscount-starttime = 1133819131268
		$server.jvm.class-loading-system.loaded class count-unit = \\ count$
		server.jvm.class-loading-system.totalloadedclasscount-count = 10285
		server.jvm.class-loading-system.totalloadedclasscount-descrip = No Description was available
		server.jvm.class-loading-system.totalloadedclasscount-lastsam = 1133819508972
		server.jvm.class-loading-system.totalloadedclasscount-name = TotalLoadedClassCount?
		server.jvm.class-loading-system.totalloadedclasscount-starttin = 1133819131268
		server.jvm.class-loading-system.totalloadedclasscount-unit = count
		server.jvm.class-loading-system.unloadedclasscount-count = 2957
		server.jvm.class-loading-system.unloadedclasscount-descriptio = No Description was available
		server.jvm.class-loading-system.unloadedclasscount-lastsamp. = 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.
		atouth at any output data mount haven your anning trailer

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. The HTTP/S port for administration. This is the port to -p --port which you should point your browser in order to manage the domain. For example, http://localhost:4848. The default port number is 4848. -s --secure If set to true, uses SSL/TLS to communicate with the domain administration server. The authorized domain administration server -u -- user 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, including the full path, 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

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin

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.

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--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
```

```
EXAMPLE 1 Using list to view all dotted-name prefixes
                                                  (Continued)
server.iiop-service.iiop-listener.SSL MUTUALAUTH.ssl
server.iiop-service.iiop-listener.orb-listener-1
server.iiop-service.orb
server.java-config
server.ims-service
server.jms-service.jms-host.default JMS host
server.log-service
server.log-service.module-log-levels
server.mdb-container
server.monitoring-service
server.monitoring-service.module-monitoring-levels
server.resource-ref.jdbc/PointBase
server.resource-ref.jdbc/ TimerPool
server.resources
server.resources.jdbc-connection-pool.PointBasePool
server.resources.idbc-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

error in executing the command

See Also get(1), set(1)

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 Access Control List page

Equivalent

Name list-admin-objects – gets all the administered objects

Synopsis list-admin-objects

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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. 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

--help

Operands target

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-application-refs – lists the existing application references

Synopsis list-application-refs

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[target]
```

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> The list-application-refs command lists all application references in a cluster or an unclustered server instance. This effectively lists all the modules deployed on the specified target (for example, J2EE applications, Web modules, and enterprise bean modules).

> The target instance or instances making up the cluster need not be running or available for this command to succeed.

This command is supported in remote mode only.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The target for which you are listing the application references. Valid values are

 server, which lists the application references for the default server instance server and is the default value

--help

Operands target

- *cluster_name*, which lists the application references for every server instance in the cluster
- instance_name, which lists the application references for the named unclustered server instance

Examples EXAMPLE 1 Using the list-application-refs command

The following command lists the application references for the unclustered server instance NewServer.

```
asadmin> list-application-refs --user admin2
--passwordfile passwords.txt NewServer
ClientSessionMDBApp
MEjbApp
__ejb_container_timer_app
Command list-application-refs executed successfully.
```

Exit Status 0 command executed successfully

1 error in executing the command

See Also create-application-ref(1), delete-application-ref(1)

Name list-audit-modules – gets all audit modules and displays them

Synopsis list-audit-modules

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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.

The HTTP/S port for administration. This is the port to -p --port

which you should point your browser in order to manage the

domain. For example, http://localhost:4848.

The default port number is 4848.

-s --secure If set to true, uses SSL/TLS to communicate with the domain

administration server.

The authorized domain administration server -u --user

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, including

> the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target on which you are listing the audit modules. Valid values are:

- server, which lists the audit modules for the default server instance server and is the default value
- *configuration_name*, which lists the audit modules for the named configuration
- cluster_name, which lists the audit modules for every server instance in the cluster
- instance_name, which lists the audit modules for a particular server instance

--help

Operands target

Examples EXAMPLE 1 Using the list-audit-modules command

```
asadmin> list-audit-modules --user admin1
--passwordfile passwords.txt --host pigeon --port 5001
```

EXAMPLE 1 Using the list-audit-modules command (Continued)

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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

Operands target_name

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.z

Date and time backup was performed: Wed Jan 11 17:50:07 PST 2006

Domains Directory: /opt/SUNWappserver/nondefaultdomaindir

Domain Directory: /opt/SUNWappserver/nondefaultdomaindir/domain1

Domain Name: domain1

Name of the user that performed the backup: jondoe The command list-backups executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also backup-domain(1), restore-domain(1)

Name list-clusters – lists the existing clusters

Synopsis list-clusters

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[target]
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

The list-clusters command lists the existing clusters.

This command is supported in remote mode only.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target for which the clusters are to be listed. Valid values are:

- domain, which lists all clusters in the domain and is the default value
- *cluster name*, which lists the named cluster
- instance_name, which lists the cluster associated with the clustered server instance. Unlike many of the other uses of instance_name, this is one situation where an unclustered instance cannot be specified.

--help

Operands target

 node_agent_name, which lists all clusters associated with the named node agent. For example, if agent1 manages server1 and server2, which are part of cluster1 and cluster2, then cluster1 and cluster2 will be listed.

Examples EXAMPLE 1 Using the list-clusters command

The following command lists all clusters in the current domain.

asadmin> list-clusters --user admin1
--passwordfile passwords.txt

MyCluster not running

Command list-clusters executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also create-cluster(1), delete-cluster(1), start-cluster(1), stop-cluster(1)

Name list-components – lists deployed components

Synopsis list-components

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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.

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 is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

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

-p --port

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--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

Examples EXAMPLE 1 Using list-components command

asadmin> list-components --user admin --passwordfile password.txt --type connector cciblackbox-tx connector-module
Command list-components executed successfully

Note: cciblackbox-tx.rar was deployed.

Exit Status 0 command executed successfully

1 error in executing the command

See Also show-component-status(1), list-sub-components(1)

Name list-configs – lists all existing configurations

Synopsis list-configs

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile *filename*] [--help]

[target]

Description Use the list—configs command to list all existing configurations in 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.

-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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This operand specifies which configurations you can list. Valid values are:

- domain, which lists the configurations in the current domain and is the default.
- *cluster_name*, which lists the configurations referenced by a cluster.
- instance_name, which lists the configuration referenced by a particular instance.

Examples EXAMPLE 1 Using the list-configs command

```
asadmin> list-configs --user admin --passwordfile passwords.txt
server-config
default-config
my-config
Command list-configs executed successfully.
```

--help

Operands target

Application Server 9.1 Section 1: Administration Commands

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

See Also delete-config(1), copy-config(1)

Name list-connector-connection-pools – gets connector connection pools that have been created

Synopsis list-connector-connection-pools

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
```

Description Use this command to list connection pools that have been created.

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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

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

asadmin> list-connector-connection-pools --user admin --passwordfile filename ims/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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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 is 4848.

-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.

The --passwordfile option specifies the name, including

the full path, 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:

--passwordfile

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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 valid in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile.

--help

Operands target

```
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-maps – lists the security maps belonging to the specified connector connection pool

```
Synopsis list-connector-security-maps
          [--terse={true|false}][ --echo={true|false} ]
          [ --interactive={true|false} ] [ --host host]
          [--port port] [--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 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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--verhose

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.
```

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

Operands target

This operand specifies the location of the custom resources. 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 a domain whose profile is the developer profile.

```
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 with a target

The following example displays the usage of this command in a domain whose profile is the cluster profile or the enterprise profile.

```
asadmin> list-custom-resources --user admin --passwordfile passwords.txt --host plum --port 4848 target6 sample_custom_resource03
```

EXAMPLE 2 Using the list-custom-resources command with a target (Continued)

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]

Description Use the list-domains command to list the domain. If the domain directory is not specified,

the domain in the default <code>install_dir/domains</code> directory is listed. If there is more that one

domain, the *domain_name* operand must be identified.

Options --domaindir The directory where the domains are to be started. If

specified, the path must be accessible in the filesystem. If not specified, the domain in the default <code>install_dir/domains</code>

directory is started.

-t -- terse Indicates that any output data must be very concise, typically

avoiding human-friendly sentences and favoring

well-formatted data for consumption by a script. Default is

false.

-e --echo Setting to true will echo the command line statement on to

the standard output. Default is false.

Examples EXAMPLE 1 Using the list-domains command

asadmin> **list-domains**

domain1 running

sampleDomain not running

Command list-domains executed successfully

Where: domain1 and sampleDomain are the domains located in the default

install dir/domains directory.

Exit Status 0 command executed successfully

1 error in executing the command

See Also create-domain(1), delete-domain(1), start-domain(1), stop-domain(1),

Name list-file-groups – lists file groups

Synopsis list-file-groups

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Identifies the name of the file user for whom the groups will be listed.

Name, in the domain.xml file, where you have different stores for file auth realm.

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.

--help

--name

--authrealmname

Operands target

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

Name list-file-users – lists the file users **Synopsis** list-file-users [--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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. The HTTP/S port for administration. This is the port to -p --port which you should point your browser in order to manage the domain. For example, http://localhost:4848. The default port number is 4848. If set to true, uses SSL/TLS to communicate with the domain -s --secure administration server. The authorized domain administration server -u --user 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.

The --passwordfile option specifies the name, including the full path, 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.

--passwordfile

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target on which you are creating the file user. This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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.

--help

Operands target

```
Examples EXAMPLE 1 Using the list-file-users command

asadmin> list-file-users instancel --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-lb-configs – lists load balancer configurations

Synopsis list-http-lb-configs

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [target]

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> Use the list-http-lb-configs command to list the load balancer configurations. List them all or list them by the cluster or server instance they reference.

		•
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.

The -- passwordfile option specifies the name, including

the full path, of a file containing the password entries in a

--passwordfile

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Lists the load balancers by target. Valid values are:

- cluster_name, which lists the load balancer configurations for this cluster.
- *instance_name*, which lists the load balancer configurations for this instance.

Examples EXAMPLE 1 Using the list-http-lb-configs command without a target

asadmin> list-http-lb-configs --user admin --passwordfile file
mycluster-http-lb-config

--help

Operands target

EXAMPLE 1 Using the list-http-lb-configs command without a target (Continued)

serverinstlb

Command list-http-lb-configs executed successfully.

EXAMPLE 2 Using the list-http-lb-configs command with the target operand.

asadmin> list-http-lb-configs --user admin --passwordfile file mycluster

mycluster-http-lb-config

Command list-http-lb-configs executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also delete-http-lb-config(1), create-http-lb-config(1)

Name list-http-lbs – lists load balancers

Synopsis list-http-lbs

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help]

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

Use the list-http-lbs command to list physical load balancers.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

```
Examples EXAMPLE 1 Using the list-http-lb-configs command
```

asadmin> list-http-lbs --user admin --passwordfile password.txt
lb1
lb2
Command list-http-lbs executed successfully.

Exit Status 0

command executed successfully

1

error in executing the command

See Also create-http-lb(1), delete-http-lb(1)

Name list-http-listeners – lists the existing HTTP listeners

Synopsis list-http-listeners

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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

--help **Operands** target

• *instance_name*, which lists the listeners for a particular server instance

Examples EXAMPLE 1 Using the list-http-listeners command

See Also create-http-listener(1), delete-http-listener(1)

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
```

Name list-iiop-listeners – lists the existing IIOP listeners

Synopsis list-iiop-listeners

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile *filename*] [--help]

[target]

 $\textbf{Description} \quad \text{The list-iiop-listeners command lists the existing IIOP listeners. This command is} \\$

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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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

--help

Operands target

• *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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[target]
```

Description Use the list-instances to list all the instances in a server. 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 is 4848.

-s --secure

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

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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--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:

```
asadmin> list-instances --user admin --passwordfile passwords.txt
--host pigeon --port 4848
il not running
i2 not running
Command list-instances executed successfully.
```

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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile *filename*] [--help]

[target]

 $\textbf{Description} \quad \text{The command lists the existing JavaMail session resources. This command is supported in } \\$

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 is 4848.

-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, including

the full path, 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

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

Examples EXAMPLE 1 Using the list-javamail-resources command

The following command lists the JavaMail session resources for the server instance:

--help

Operands target

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-jbi-binding-components – lists the binding components installed on the specified target

Synopsis list-jbi-binding-components

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

[--lifecyclestate shutdown|started|stopped]

[--libraryname shared_library_name] [--assemblyname service assembly name]

[--target *target*]

Description The list-jbi-binding-components command lists all the binding components installed on the specified target. If no filters are specified, the command lists all the components installed on the target.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Helps list the JBI binding components based on its current state. For example, if you want to list only those binding components that are started, you can specify the option —lifecyclestate with the value as started. By default, all JBI binding components are listed, regardless of their states. Valid values for this option are:

 shutdown, which lists all the JBI binding components that are currently shutdown on the specified target.

--help

--lifecyclestate

--libraryname

--assemblyname

--target

- started, which lists all the JBI binding components that are in the 'started' state on the specified target.
- stopped, which lists all the JBI binding components on the specified target that are not running.

Helps list the JBI binding components that currently use the specified library.

Helps list the JBI binding components that have a service unit deployed as part of the service assembly unit with the specified service assembly name.

Specifies the target for which you want to list the JBI binding components. Specify this option only if the binding components are deployed in a multiserver environment with a Domain Administration Server (DAS). If the binding components are not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which lists the binding components on the embedded DAS instance. This is the default value.
- domain, which lists the binding components for the administrative domain itself. Specify domain only if you are using the cluster profile.
- cluster_name, which lists the binding component for every server instance in the cluster
- instance_name, which lists the binding components for the named unclustered server instance.

Examples EXAMPLE 1 Using the list-jbi-binding-components command

The following command lists the JBI binding components.

```
asadmin> list-jbi-binding-components --user admin2
--passwordfile passwords.txt --lifecyclestate started
--libraryname library1 --target server1
Command list-jbi-binding-components executed successfully.
```

Exit Status 0

command executed successfully

1 error in executing the command

See Also install-jbi-component(1), delete-application-ref(1), delete-application-ref(1), delete-application-ref(1)

514

Name list-jbi-service-assemblies – lists the service assemblies installed into the JBI environment

Synopsis list-jbi-service-assemblies

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user]

[--passwordfile *filename*] [--help]

[--lifecyclestate shutdown|started|stopped]

[--componentname component_name] [--target target]

Description The list-jbi-service-assemblies command lists the service assemblies deployed into the JBI environment. If no filters are specified, the command will list all the deployed service assemblies.

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.

Setting to true will echo the command line statement on the -e --echo

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.

The HTTP/S port for administration. This is the port to -p --port

which you should point your browser in order to manage the

domain. For example, http://localhost:4848.

The default port number is 4848.

-s --secure If set to true, uses SSL/TLS to communicate with the domain

administration server.

The authorized domain administration server -u --user

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, including

> the full path, 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

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Helps list the service assemblies based on its current state. For example, if you want to list only those service assemblies that are started, you can specify the option —lifecyclestate with the value as started. By default, all service assemblies are listed, regardless of their states. Valid values for this option are:

- shutdown, which lists all the service assemblies that are currently shut down.
- started, which lists all the service assemblies that are in the 'started' state on the specified target.
- stopped, which lists all the service assemblies on the specified target that are not running.

--help

--lifecyclestate

--target

Specifies the target for which you want to list the JBI service assemblies. Specify this option only if the service assemblies are deployed in a multiserver environment with a Domain Administration Server (DAS). If the service assemblies are not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which lists the service assemblies on the embedded DAS instance. This is the default value.
- domain, which lists the service assemblies for the administrative domain itself. Specify domain only if you are using the cluster profile.
- *cluster name*, which lists the service assemblies for every server instance in the cluster.
- *instance name*, which lists the service assemblies for the named unclustered server instance.

--componentname

Specifies the name of the component for which you want to list the IBI service assemblies.

Examples EXAMPLE 1 Using the list-jbi-service-assemblies command

The following command lists the JBI service assemblies.

```
asadmin> list-jbi-service-assemblies --user admin2
--passwordfile passwords.txt --componentname component_name
--target server1
Command list-jbi-service-assemblies executed successfully.
```

Exit Status 0

command executed successfully

1

error in executing the command

See Also install-jbi-component(1), delete-application-ref(1), delete-application-ref(1), delete-application-ref(1), delete-application-ref(1)

Name list-jbi-service-engines – lists the service engines installed on the specified target

Synopsis list-jbi-service-engines

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

[--lifecyclestate shutdown|started|stopped]

[--libraryname shared_library_name]
[--assemblyname service assembly name]

[--target *target*]

Description The list-jbi-service-engines command lists the service engines installed on the specified target. If no filters are specified, the command will list all the installed service engines.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Helps list the service engines based on its current state. For example, if you want to list only those service engines that are started, you can specify -lifecyclestate started. By default, all service engines are listed, regardless of their states. Valid values for this option are:

- shutdown, which lists all the service engines that are currently shutdown on the specified target.
- started, which lists all the service engines that are in the 'started' state on the specified target.

--help

--lifecyclestate

--libraryname

--assemblyname

--target

stopped, which lists all the service engines on the specified target that are not running.

Helps list the service engines that currently use the specified library.

Helps list the service engines that have a service unit deployed as part of the service assembly unit with the specified service assembly name.

Specifies the target for which you want to list the JBI service engines. Specify this option only if the service engines are deployed in a multiserver environment with a Domain Administration Server (DAS). If the service engines are not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which lists the service engines on the embedded DAS instance. This is the default value.
- domain, which lists the service engines for the administrative domain itself. Specify domain only if you are using the cluster profile.
- cluster_name, which lists the service engines for every server instance in the cluster.
- *instance name*, which lists the service engines for the named unclustered server instance.

Examples EXAMPLE 1 Using the list-jbi-service-engines command

The following command lists the JBI service engines.

```
asadmin> list-jbi-service-engines --user admin2
--passwordfile passwords.txt --lifecyclestate started
--assemblyname serviceassembly1 --target server1
Command list-jbi-service-engines executed successfully.
```

Exit Status 0

command executed successfully

error in executing the command

See Also install-jbi-component(1), delete-application-ref(1), delete-application-ref(1), delete-application-ref(1), delete-application-ref(1)

Name list-jbi-shared-libraries – lists the JBI shared libraries that are installed into the JBI environment

Synopsis list-jbi-shared-libraries

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [--target target] [--componentname componentname]

Options -t--terse

Description The list-jbi-shared-libraries command lists the JBI shared libraries that are installed on the specified target. If no target is specified, the command lists all JBI shared libraries that are installed in the JBI environment.

Indicates that any output data must be very concise, typically

·		avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-e	echo	Setting to true will echo the 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 is 4848.
- 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 theuser option on subsequent operations to this particular domain.
p	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target for which you want to list the JBI shared libraries. Specify this option only if the shared libraries are installed in a multiserver environment with a Domain Administration Server (DAS). If the shared libraries are not installed in a multiserver environment with a DAS, this option is ignored. Valid values are:

 server, which lists the JBI shared libraries on the embedded DAS instance. This is the default value.

--help

--target

- domain, which lists the JBI shared libraries for the administrative domain itself. Specify domain only if you are using the cluster profile.
- cluster_name, which lists the JBI shared libraries on every server instance in the cluster.
- *instance_name*, which lists the JBI shared libraries on the named unclustered server instance.

--componentname

Helps list the shared libraries referenced by the specified component.

Examples EXAMPLE 1 Using the list-jbi-shared-libraries command

The following command lists the JBI shared libraries on the specified server instance.

```
asadmin> list-jbi-shared-libraries --user admin2
--passwordfile passwords.txt --target server1
Command list-jbi-shared-libraries executed successfully.
```

Exit Status 0

command executed successfully

1

error in executing the command

See Also show-jbi-shared-library(1), install-jbi-shared-library(1)

Name list-jdbc-connection-pools – lists all JDBC connection pools

Synopsis list-jdbc-connection-pools

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

[target]

--passwordfile

 $\textbf{Description} \quad \text{The list-jdbc-resources command displays a list of JDBC resources that have been} \\$

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 is 4848.

-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.

option on subsequent operations to this particular domain.

The --passwordfile option specifies the name, including the full path, 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

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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.

--help

Operands target

Examples EXAMPLE 1 Using the list-jdbc-resources command

 $\verb|asadmin>| \textbf{list-jdbc-resources}| \textbf{ --user}| \textbf{ admin}| \textbf{ --passwordfile}| \textbf{ passwords.txt}|$

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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]
[--passwordfile filename] [--help]

[--passwordille juename]

[--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 is 4848.

-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, including

the full path, 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

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The type of JMS destinations to be listed. Valid values are topic and queue.

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

--help

-T--desttype

Operands target

- *cluster_name*, which lists the physical destinations for the specified cluster
- *instance_name*, which lists the physical destinations for a particular server instance

Examples EXAMPLE 1 Using the list-jmsdest command

The following command lists all the physical destinations for the default server instance:

```
asadmin> list-jmsdest --user admin
           --passwordfile passwords.txt --host bluestar --port 4848
           PhysicalQueue queue {}
           PhysicalTopic topic {}
           Command list-jmsdest executed successfully.
Exit Status 0
                                          command executed successfully
```

1 error in executing the command

See Also create-jmsdest(1), delete-jmsdest(1)

Name list-jms-hosts – lists the existing JMS hosts

Synopsis list-jms-hosts

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile *filename*] [--help]

[target]

 $\textbf{Description} \quad \text{The list-jms-hosts command lists the existing JMS hosts for the JMS service. This is the existing JMS hosts for the JMS service and the list-jms-hosts command lists the existing JMS hosts for the JMS service. This is the existing JMS hosts for the JMS service and the list-jms-hosts command lists the existing JMS hosts for the JMS service. This is the existing JMS hosts for the JMS service and the list-jms-hosts command lists the existing JMS hosts for the JMS service. This is the existing JMS hosts for the JMS service and the list-jms-hosts command lists the existing JMS hosts for the JMS service. This is the existing JMS hosts for the JMS service and the list-jms-hosts for the list-jms-hosts f$

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 is 4848.

-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, including

the full path, 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

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This operand specifies the target for which the JMS hosts are to be listed. Valid values are:

- server, which lists the JMS hosts for the default server instance and is the default value
- configuration_name, which lists the JMS hosts for the specified configuration
- cluster_name, which lists the JMS hosts for the specified cluster
- instance_name, which lists the JMS hosts for a particular server instance

--help

Operands target

Examples EXAMPLE 1 Using the list-jms-hosts command

The following command lists the JMS hosts for the server configuration.

asadmin> list-jms-hosts --user admin
--passwordfile passwords.txt server-config
default_JMS_host
MyNewHost
Command list-jms-hosts executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also create-jms-host(1), delete-jms-host(1)

Name list-jms-resources – lists the JMS resources

Synopsis list-jms-resources

-p --port

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.	
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.	
	-Iinteractive	If set to true (default), only the required password options are prompted.	
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.	

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 is 4848.

-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, including

the full path, 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

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The JMS resource type can be javax.jms.Topic, javax.jms.Queue, javax.jms.TopicConnectionFactory, or javax.jms.QueueConnectionFactory.

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.

--help

--restype

Operands target

```
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
            ims/Topic
            jms/QueueConnectionFactory
            jms/DurableTopicConnectionFactory
            Command list-jms-resources executed successfully.
           EXAMPLE 2 Using the list-jms-resources command to list JMS resources of a specified type
            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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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 is 4848.

-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, including

the full path, 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

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--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 "server," "domain," cluster, or instance.

Examples EXAMPLE 1 Using the list-jndi-entries command

```
asadmin> list-jndi-entries --user admin1 --passwordfile adminadmin1
  --host plum --port 5001 target1
jndi_entry03
jndi_entry72
jndi_entry76
```

EXAMPLE 1 Using the list-jndi-entries command (Continued)

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-indi-resources

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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

-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 is 4848.

-s --secure

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

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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--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

Examples EXAMPLE 1 Using the list-jndi-resources command

The following is an example of using the list-jndi-resources command in a domain whose profile is the developer profile.

```
asadmin> list-jndi-resources --user admin
--passwordfile passwords.txt --host plum
jndi_resource1
jndi_resource2
jndi_resource3
Command list-jndi-resources executed successfully
```

The following is an example of using the list-jndi-resources command in a domain whose profile is the cluster profile or the enterprise profile.

```
asadmin> list-jndi-resources --user admin --passwordfile
passwords.txt --host plum --port 4848 instance1
jndi_resource1
jndi_resource2
```

EXAMPLE 1 Using the list-jndi-resources command (Continued)

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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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.

	server environment. This communicates supported in remote mode only.	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, of a file containing the password entries in a

uppercase letters.

specific format. The entry for the password must have the AS ADMIN prefix followed by the password name in

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option indicates the location where the lifecycle module exists. The valid targets for this command are configuration, instance, cluster, or server.

--help

Operands target

Examples EXAMPLE 1 Using list-lifecycle-modules:

asadmin> list-lifecycle-modules --user admin
--passwordfile adminpassword.txt --host fuyako --port 7070
JBIFramework
WSTCPConnectorLCModule
Command list-lifecycle-modules executed successfully

Where JBI Framework and WSTCPConnectorLCModule are the lifecycle modules listed for the default target, server.

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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

myRulel

--help

Operands target

Command list-management-rules executed successfully

Exit Status 0 command executed successfully

1 error in executing the command

See Also delete-lifecycle-module(1), list-lifecycle-modules(1)

Name list-mbeans – lists the custom mbeans for a given target server instance.

Synopsis list-mbeans

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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.

-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
-Iinteractive	If set to true (default), only the required password options are prompted.
-Hhost	The machine name where the domain administration server is running. The default value is localhost.
-pport	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 is 4848.
-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for ${\sf AS_ADMIN_MASTERPASSWORD}$ is changeit.

Displays the help text for the command.

The target for the MBean. Identifies the server instance. Defaults to the name of the Domain Adminstration Server (DAS).

--help

Operands -target=server

Examples EXAMPLE 1 Using list-mbeans

asadmin>list-mbeans target=server1

mbeanFoo

Command list-mbeans executed successfuly

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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.

-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
-Iinteractive	If set to true (default), only the required password options are prompted.
-Hhost	The machine name where the domain administration server is running. The default value is localhost.
-pport	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 is 4848.
-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
-uuser	The authorized domain administration server administrative username.
	If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.

--passwordfile

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The message-layer for which the provider has to be listed. The default value is SOAP.

This operand is valid in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. Lists all the objects of the specified type in the named configuration referenced by the named server instance or cluster. Valid values include:

--help

--layer

Operands target

- server, which deploys the component to the default server instance server and is the default value
- config, which deploys the component to the domain.
- cluster, which deploys the component to every server instance in the cluster.
- instance, which deploys the component to a particular server instance.

Examples EXAMPLE 1 Using list-message-security-providers

The following example shows how to list message security providers for a message layer.

asadmin> list-message-security-providers --user admin

--layer SOAP

XWS ClientProvider

ClientProvider

XWS ServerProvider ServerProvider

Command list-message-security-providers executed successfully.

Exit Status 0

command executed successfully

1

error in executing the command

See Also create-message-security-provider(1), delete-message-security-provider(1)

Name list-node-agents – lists the node agents along with their status

Synopsis list-node-agents

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [target]

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> This command displays the node agents along with their status (for example, running or stopped). To list all node agents, omit the target.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.

The -- passwordfile option specifies the name, including

the full path, of a file containing the password entries in a

--passwordfile

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This operand specifies which node agents are to be listed. The options are:

- domain Domain is the default. It lists all of the node agents in the domain.
- cluster_name This lists all of the node agents associated with the named cluster.
- *instance_name* This lists all of the node agents associated with the named server instance.

--help

Operands target

• *agent_name* This lists the named node agent.

Examples EXAMPLE 1 Using list-node-agents

asadmin>list-node-agents --user admin1 --passwordfile filename

agent1 not running

Command list-node-agents executed successfully.

Where: agent1 is the only node agent in the domain.

Exit Status 0 command executed successfully

1 error in executing the command

See Also create-node-agent(1), delete-node-agent(1), start-node-agent(1), stop-node-agent(1)

Name list-password-aliases – lists all password aliases

Synopsis list-password-aliases

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user]

[--passwordfile *filename*] [--help]

Description This command lists all of the password aliases.

A	T 101 .	. 1	11
Options -tterse	Indicates that any output	t data must be verv	concise, typically

avoiding human-friendly sentences and favoring

well-formatted data for consumption by a script. Default is

false.

-e --echo Setting to true will echo the 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.

The HTTP/S port for administration. This is the port to -p --port

which you should point your browser in order to manage the

domain. For example, http://localhost:4848.

The default port number is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

administration server.

The authorized domain administration server -u --user

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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--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 ${\tt jmspassword-alias}$

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

--passwordfile

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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 is 4848.

-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.

option on subsequent operations to this particular domain.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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.

--help

Operands target

Examples EXAMPLE 1 Using list-persistence-resources

This example lists all the persistence resources.

 $\verb|asadmin>| \textbf{list-persistence-resources}| \textbf{ --user admin}|$

--passwordfile passwords.txt

 ${\tt sample_persistence_resource}$

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

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile *filename*] [--help]

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.

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 is 4848.

-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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

command executed successfully

error in executing the command

See Also publish-to-registry(1), unpublish-from-registry(1)

--help

1

Exit Status 0

Name list-resource-adapter-configs – lists the names of the resource—adapter—configs created.

Synopsis list-resource-adapter-configs

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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 -tterse	Indicates that any output data must be very concise, typically
	. 1. 1

avoiding human-friendly sentences and favoring

well-formatted data for consumption by a script. Default is

false.

-e --echo Setting to true will echo the command line statement on the

standard output. Default is false.

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

are prompted.

The machine name where the domain administration server -H --host

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 is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

administration server.

The authorized domain administration server -u --user

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, including

> the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option helps to list the properties that are configured.

This option lists the connector module name.

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

--help

--verbose

--raname

Operands target

ra2

566

EXAMPLE 1 Using the list-resource-adapter-configs command (Continued)

Command list-resource-adapter-configs executed successfully

Exit Status 0 command executed successfully

1 error in executing the command

See Also create-resource-adapter-config(1), delete-resource-adapter-config(1)

Name list-resource-refs – lists the existing resource references

Synopsis list-resource-refs

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[target]
```

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> The list-resource-refs command lists all resource references in a cluster or an unclustered server instance. This effectively lists all the resources (for example, JDBC resources) available in the JNDI tree of the specified target.

The target instance or instances making up the cluster need not be running or available for this command to succeed.

This command is supported in remote mode only.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The target for which you are listing the resource references. Valid targets are

 server, which lists the resource references for the default server instance and is the default target.

--help

Operands target

- cluster_name, which lists the resource references for every server instance in the cluster
- instance_name, which lists the resource references for the named unclustered server instance

Examples EXAMPLE 1 Using the list-resource-refs command

The following command lists the resource references for the cluster MyCluster.

asadmin> list-resource-refs --user admin
--passwordfile passwords.txt MyCluster
jms/Topic
Command list-resource-refs executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also create-resource-ref(1), delete-resource-ref(1)

Name list-sub-components – lists EJBs or Servlets in deployed module or module of deployed application

Synopsis list-sub-components

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --type eibs|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

	supported in remote mode only.	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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,

The default port number is 4848.

http://localhost:4848.

-s --secure administration server.

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

The authorized domain administration server administrative username. -u--user

> 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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--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.

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 -module name This is the name of the module containing the sub-component.

Examples EXAMPLE 1 Using list-sub-components

-appname

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[target target_name]
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> 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.

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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--heln

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.

```
Examples EXAMPLE 1 Using list-system-properties

asadmin> list-system-properties --user admin
--passwordfile password.txt --host localhost --port 4848
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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

Operands target

Examples EXAMPLE 1 Using list-threadpools

asadmin> list-threadpools --user admin --passwordfile password.txt threadpool-1

EXAMPLE 1 Using list-threadpools (Continued)

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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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.

	supported in remote mode only.	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, of a file containing the password entries in a specific format. The entry for the password must have the

uppercase letters.

AS ADMIN prefix followed by the password name in

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

Operands target

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

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]
[--passwordfile filename] [--help]
[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.

webservice name option is omitted, then all the transformation rules will be listed. 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. The machine name where the domain administration server. -H --host 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 is 4848.

-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, including

the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

[target]

--passwordfile

 $\textbf{Description} \quad \text{The list-virtual-servers command lists the existing virtual servers. This command is a substitution of the list-virtual servers and the existing virtual servers are substituted as the existing virtual servers. This command is the existing virtual servers are substituted as the existing virtual servers. This command is the existing virtual servers are substituted as the existing virtual servers. This command is the existing virtual servers are substituted as the existing virtual servers. The existing virtual servers are substituted as the existing virtual servers are substituted as the existing virtual servers. The existing virtual servers are substituted as the existing virtual servers are substituted as the existing virtual servers. The existing virtual servers are substituted as the existing virtual servers are$

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 is 4848.

-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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

Operands target

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

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

 $asadmin{>} \mbox{deploy}$ --user admin --passwordfile passwordfile.txt <other options> /home/myapplication.ear

 $as admin \verb|-list-components| -- user admin| -- password file| password file.txt| < other options \verb|-$

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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Hhost	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.
	-pport	The port number of the domain administration server listening for administration requests.
	-ssecure	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.
```

EXAMPLE 1 Using the login command (Continued)

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 migrate-timers – moves a timer when a server instance stops

Synopsis migrate-timers

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
 [ --destination destination_server_name]
server name
```

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> The function of the migrate-timers command is to move the timer to a specified server, when the server instance stops or fails abnormally. This command is supported in remote mode only.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This is the destination server instance. If this option is not specified, then DAS will find a server instance or multiple server instances. A migration notification will be sent to the selected server instances.

This is the current location of the server instance. The server instance should not be active during this process.

--help

--destination

Operands server_name

Examples EXAMPLE 1 Using migrate-timers

This is a simple example of how to use the command.

 $\verb|asadmin>| \verb|migrate-timers| --server name| dance|$

This command was successfully executed.

Exit Status 0 command executed successfully

1 error in executing the command

See Also list-timers(1)

Name monitor – displays monitoring data for commonly-used Application Server components

Synopsis monitor

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile *filename*] [--help] --type monitor_type [--filename file_name] [--interval interval] [--filter_filter_name] instance name

Description This command prints out commonly-monitored attributes of Application Server components, and has options for filtering out statistics and capturing the output in a Comma Separated Values (CSV) file. The output appears in a table format. To view the legend of the table header, type h.

> Note – To monitor information for a given attribute, the attribute's monitoring level must be set to HIGH or LOW. Set the monitoring level through the Admin Console, or use the set command.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The type of statistics to monitor. Valid values are:

- connection
- connectionqueue
- connectorpool
- endpoint
- entitybean
- filecache

--help

--type

- httplistener
- httpservice
- jdbcpool
- jvm
- keepalive
- messagedriven
- servlet
- statefulsession
- statelesssession
- threadpool
- webmodule

--filename Saves output to a file in CSV format.

--interval The interval in seconds before capturing monitoring attributes. If the interval must be greater than 0. The monitoring attributes are displayed on stdout until you type

ctrl-c or q. The default value is 30.

--filter If there is more than one monitorable element in the given

type, use this option to filter the results to get the

information you want.

Operands *instance_name* The server instance for which to view monitoring data.

Examples For the following examples, enable monitoring for the type before running the commands. For example:

asadmin set server.monitoring-service.module-monitoring-levels.jvm=LOW

EXAMPLE 1 Sending output to the screen:

asadmin> monitor --type jvm --user admin --passwordfile password.txt server

JVM Monitoring

EXAMPLE 2 Using the filter option:

The following example shows a type for which there are multiple monitoring options when the filter option is not used:

asadmin> monitor --type httplistener --user admin --passwordfile password.txt server

There are more than one monitoring elements. Please consider using the filter option. The following are available elements to monitor:

http-listener-1

```
EXAMPLE 2 Using the filter option: (Continued)
```

```
http-listener-2
CLI137 Command monitor failed.
```

Using the filter option:

```
asadmin> monitor --type httplistener --filter http-listener-1
--user admin --passwordfile password.txt server
```

```
HTTP Listener Monitoring: http-listener-1
hr
          c200 c2xx c302 c304 c3xx c400 c401 c403 c404 c4xx c503 c5xx coc co
ctc
     ctb
                moc
                     mst.
                          m†
                                m†m
                                     mc+
                                          pt
                                                rc
     0
          Ø
                     0
                          3
                                3
                                                0
2
                                     2
                                                3
          a
                1
                     20
                          20
                                2
                                           6
```

Enter h to see the legend for the table headings:

```
= Cumulative value of the Bytes received by each of the Request Processors
      = Cumulative value of the Bytes sent by each of the Request Processors
* c200 = Number of responses with a status code equal to 200
* c2xx = Number of responses with a status code in the 2xx range
* c302 = Number of responses with a status code equal to 302
* c304 = Number of responses with a status code equal to 304
* c3xx = Number of responses with a status code in the 3xx range
* c400 = Number of responses with a status code equal to 400
* c401 = Number of responses with a status code equal to 401
* c403 = Number of responses with a status code equal to 403
* c404 = Number of responses with a status code equal to 404
* c4xx = Number of responses with a status code equal to 4xx
* c504 = Number of responses with a status code equal to 504
* c5xx = Number of responses with a status code equal to 5xx
* coc = Number of open connections
     = Number of responses with a status code outside the 2xx, 3xx, 4xx, and 5xx range *
* ctc = Number of request processing threads currently in the listener thread pool
* ctb = Number of request processing threads currently in use in the listener thread
         pool serving requests
      = Number of responses with a status code equal to 400
* moc = Maximum number of open connections
st mst \,=\, Minimum number of request processing threads that will be created at listener
         startup time and maintained as spare threads above the current thread count
* mt
      = Maximum number of request processing threads that are created by the listener
 mtm = Provides the longest response time for a request - not a cumulative value, but
         the largest response time from among the response times
      = Cumulative value of the times taken to process each request. The processing
         time is the average of request processing times over the request count
      = Cumulative number of the requests processed so far
```

EXAMPLE 2 Using the filter option: (Continued)

Exit Status 0 command executed successfully

1 error in executing the command

See Also get(1), list(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=fa

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.

reads the commands as defined in the file. Options --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.

indicates that any output data must be very concise, typically --terse

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 ping-connection-pool – tests if a connection pool is usable

Synopsis ping-connection-pool

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option is deprecated.

This is the name of the pool to test.

--help

--target

Operands pool_name

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_list

--webservicename qualified_webservice_name

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

--lbhost loadbalancer_host--lbport lb_port--lbsslport loadbalancer_secure_port--organization organization

--description description

Description Publishes the web service artifacts to registries.

Options --registryindinames

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

-t --terse

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.

-e --echo

Setting to true will echo the 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 is 4848.

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

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.

The --passwordfile option specifies the name, including the full path, 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.

-s --secure

-u--user

--passwordfile

The default value for AS_ADMIN_MASTERPASSWORD is

changeit.

--help Displays the help text for the command.

--lbhost Specifies the load balancer host.--lbport Specifies the load balancer port.

--lbsslport Specifies the load balancer secure port.

--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#myMod

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

-p --port

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]
[--passwordfile filename] [--help]
[--txlogdir transaction_log_dir] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server

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

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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--help

--transactionlogdir

Displays the help text for the command.

When a server fails it writes the location in its transaction log. If the failed server's transaction logs are copied to some other location to make it available to the surrogate recovery server, this option should be used. If the failed server's transaction-service, tx-log-dir is modified to reflect a new location, then this option is not required.

--destination

the name of the destination server to which the pending transactions need to be recovered.

Operands server_name

This is the name of the server that failed. It is this server that is hosting the transaction that will be recovered.

Examples EXAMPLE 1 Using recover-transactions

asadmin>recover-transactions sampleserver

Transaction recovered.

Exit Status 0 command executed successfully

1 error in executing the command

Name remove-ha-cluster – returns an HA cluster to non-HA status

Synopsis remove-ha-cluster

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --haagentport port_number]
 [--haadminpassword password] [--hosts hadb-host-list] databaseName
```

Description Note - This command requires the HADB software. This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> This command returns an HA cluster to non-HA status. Use fully qualified hostnames when specifying the hostlist interfaces explicitly for hosts with multiple network interfaces. This command is supported in remote mode only.

The command performs the following tasks:

- The HA database is stopped.
- The HA database is deleted.
- The command deletes and/or modifies the appropriate resources in domain.xml.

Options -t--terse

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.

-e --echo

Setting to true will echo the 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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--haagentport

This is the HA agent port containing the cluster to be changed. The default value is 1862.

--haadminpassword

This is the HA administrator's password.

--hosts

This is a list of comma separated host names where the HADB instance is configured. The number of hosts must be greater than 1 and must be an even number. The same host names can be repeated. Use fully qualified hostnames when specifying the hostlist interfaces explicitly for hosts with multiple network interfaces.

Operands databasename

This is the name of the database to be removed.

Examples EXAMPLE 1 Using remove-ha-cluster

asadmin> remove-ha-cluster --user u1 paswordfile pfile1 --haagentport 1860 cluster1

Command remove-ha-cluster executed successfully

Exit Status 0 command executed successfully

1 error in executing the command

See Also configure-ha-cluster(1)

Name restore-domain – restores files from backup

Synopsis restore-domain [--domaindir *domain_directory*]

[--filename backup_filename] [--description description]

[--terse=false] [--verbose=false]

[domain_name]

Description This command restores files under the domain from a backup directory. The restore-domain

command is supported in local mode only.

Options --domaindir This option specifies the parent directory of the domain

upon which the command will operate. The default is

install dir/domains.

--filename The restore is performed using the specified zip file as the

source.

--description A description can contain any string to help identify the

particular backup. The description is displayed as part of the

information for any backup.

-t -- terse Indicates that any output data must be very concise, typically

avoiding human-friendly sentences and favoring

well-formatted data for consumption by a script. Default is

false.

-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 Successfully restored the domain (domain1), from /opt/SUNWappserver/nondefaultdomaindir/domai

Description: 1137030607263

Backup Filename: /opt/SUNWappserver/nondefaultdomaindir/domain1/backups/sjsas_backup_v00001.z

Date and time backup was performed: Wed Jan 11 17:50:07 PST 2006

Domains Directory: /opt/SUNWappserver/nondefaultdomaindir

Domain Directory: /opt/SUNWappserver/nondefaultdomaindir/domain1

Domain Name: domain1

Name of the user that performed the backup: jondoe

Exit Status 0 command executed successfully

1 error in executing the command

See Also backup-domain(1), list-backups(1)

Name rollback-transaction – rolls back the named transaction

Synopsis rollback-transaction

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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

coci.ptioi.	is supported in remote mode only.	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.

The default port number is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

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, including

> the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

--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 or any other standalone instance

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), unfreeze-transaction-service(1)

Name set – sets the values of attributes

Synopsis set

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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.
- 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	
	<pre>default-config.admin-service</pre>	
	<pre>default-config.admin-service.das-config</pre>	
	<pre>default-config.admin-service.jmx-connector.system</pre>	
	<pre>default-config.admin-service.jmx-connector.system.ssl</pre>	
	<pre>default-config.availability-service</pre>	
	<pre>default-config.availability-service.jms-availability</pre>	
	<pre>default-config.diagnostic-service</pre>	
	<pre>default-config.ejb-container</pre>	
	•	
	<pre>default-config.http-service.http-listener.http-listener-1</pre>	
	<pre>default-config.http-service.http-listener.http-listener-2</pre>	
	•	
	<pre>default-config.iiop-service</pre>	
	•	
	<pre>default-config.java-config</pre>	
	•	
	■ domain	
	<pre>domain.clusters</pre>	
	<pre>domain.configs</pre>	
	■ domain.resources	
	<pre>domain.resources.jdbc-connection-pool.DerbyPool</pre>	
	domain.resources.jdbc-connection-poolCallFlowPool	
	<pre>domain.resources.jdbc-connection-poolTimerPool</pre>	
	•	
	■ server	
	■ server-config	
	<pre>cerver-config.admin-service</pre>	
	<pre>server-config.admin-service.das-config</pre>	
	<pre>server-config.admin-service.jmx-connector.system</pre>	
	<pre>server-config.admin-service.jmx-connector.system.ssl</pre>	
	<pre>server-config-availability-servicce</pre>	
	<pre>server-config.availability-service.jms-availability</pre>	
	<pre>server-config.diagnostic-service</pre>	
	<pre>server-config.ejb-container</pre>	
	•	
	<pre>server.log-service</pre>	
	<pre>server.log-service.module-log-levels</pre>	
	•	
	<pre>server.session-config</pre>	
	<pre>server.session-config.session-manager</pre>	
	<pre>server.session-config.session-manager.manager-properties</pre>	
	<pre>server.session-config.session-manager.store-properties</pre>	
plication Server 9.	 server.session-config.session-properties 1 Section 1: Administration Commands Server.timead-pools 	617
	■ server.thread-pools.thread-pool-1	
	35. ver rem dag poots rem dag poot rem dag poot 1	

■ server.transaction-service

Command	Output
Command list -monitor *	<pre>server server.applications server.applicationsJWSappclients server.applicationsJWSappclients.sys\.war server.applications.adminapp server.applications.admingui server.connector-service</pre>
	<pre>server.http-service server.http-service.server server.jms-service server.jvm server.orb server.orb.connection-managers server.resources server.thread-pools</pre>

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 thelist 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:

1	list "*" grep http grep listener	 default-config.http-service. http-listener.http-listener-1 default-config.http-service. http-listener.http-listener-2 server-config.http-service. http-listener.admin-listener server-config.http-service. http-listener.http-listener-1 server-config.http-service. http-listener.http-listener-2 server-thtp-service.http-listener.admin-listener server.http-service.http-listener.http-listener-1 server.http-service.http-listener.http-listener-2
2	To find the listener that corresponds to the default http-listener where the web applications in the domain/server are deployed: 1. Examine the dotted name starting with item number 7 in above output. 2. Use the get command as shown in its usage. For example, get server. http-service.http-listener.http-listener.1.* will return all the attributes of the http-listener in context.	server.http-service.http-listener.http-listener-1.acceptor-threads = 1 server.http-service.http-listener.http-listener-1.address = 0.0.0.0 server.http-service.http-listener.http-listener-1.blocking-enabled = false server.http-service.http-listener.http-listener-1.default-virtual-ser = server server.http-service.http-listener.http-listener-1.enabled = true server.http-service.http-listener.http-listener-1.external-port = server.http-service.http-listener.http-listener-1.family = inet server.http-service.http-listener.http-listener-1.id = http-listener-1 server.http-service.http-listener.http-listener-1.port = 8080 server.http-service.http-listener.http-listener-1.redirect-port = server.http-service.http-listener.http-listener-1.security-enabled = false server.http-service.http-listener.http-listener-1.server-name = server.http-service.http-listener.http-listener-1.xpowered-by = true

Output/Comment

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:

ID

Command

- 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-service server.monitoring-service.module-monitoring-levels
		Note that this is the list command. It only shows the hierarchy, nothing else. Using the ' ' and "grep" narrows down the search effectively. Now, you can choose server.monitoring-service to set the attributes of various attributes that can be monitored.
		This is the configuration data because this setting will be persisted to the server's configuration store.
2	get server.monitoring-service.*	You can try the number of attributes that are presently available with monitoring service. Here is the output:
		No matches resulted from the wildcard expression. This is because this fully dotted name does not have any attributes at all. Logically, you try the next one and that is: server.monitoring-service.module-monitoring-levels. Again, use the wildcard character to get ALL the attributes of a particular component.

ID	Command	Output/Comment
3	get server.monitoring-service. module-monitoring-levels.*	server.monitoring-service.module-monitoring-levels. connector-connection-pool = 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-pool = 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	<pre>set server.monitoring-service. module-monitoring-levels. jvm=HIGH</pre>	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	listmonitor * grep 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-	server.jvm.class-loading-system.dotted-name = server.jvm.class-loading-system
	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-lastsampletin = 1133819508973
		<pre>server.jvm.class-loading-system.loadedclasscount-name = LoadedClassCount?</pre>
		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-descripti = No Description was available
		server.jvm.class-loading-system.totalloadedclasscount-lastsamp = 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-lastsample = 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
	terse India	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. The HTTP/S port for administration. This is the port to -p --port which you should point your browser in order to manage the domain. For example, http://localhost:4848. The default port number is 4848. -s --secure If set to true, uses SSL/TLS to communicate with the domain administration server. The authorized domain administration server -u -- user 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, including the full path, 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

If you have authenticated to a domain using the asadmin login command, then you need not specify the admin

passwords, that must be specified for remote commands, use the --passwordfile or enter them at the command prompt.

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

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

--help

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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

• *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 show-jbi-binding-component – shows detailed information about the specified binding component

Synopsis show-jbi-binding-component

-u --user

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]
[--passwordfile filename] [--help]
[--target target]
component_name

Description The show-jbi-binding-component command shows details about the specified binding component.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.

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

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, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target for which you want to show details of the specified JBI binding component. Specify this option only if the binding component is deployed in a multiserver environment with a Domain Administration Server (DAS). If the binding component is not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

 server, which shows detailed information about a specified binding component on the embedded DAS instance. This is the default value.

--help

- domain, which displays detailed information about a specified binding component for the administrative domain itself. Specify domain only if you are using the cluster profile.
- cluster_name, which displays detailed information about a specified binding component on every server instance in the cluster.
- instance_name, which displays detailed information about a specified binding component on a named unclustered server instance.

Operands *component_name*

The name of the JBI binding component about which you want the detailed information.

Examples EXAMPLE 1 Using the show-jbi-binding-component command

The following command shows details of the specified JBI binding component on the server instance.

```
asadmin> show-jbi-binding-component --user admin2
--passwordfile passwords.txt --lifecyclestate started
--libraryname library1 --target server1 component1
Command show-jbi-binding-component executed successfully.
```

Exit Status 0

command executed successfully

1

error in executing the command

See Also install-jbi-component(1), list-jbi-binding-components(1), stop-jbi-component(1), delete-application-ref(1)

Name show-jbi-service-assembly - shows detailed information about a specified service assembly

Synopsis show-jbi-service-assembly

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

[--target target] service_assembly_name

Description The show-jbi-service-assembly command displays detailed information about a specified

service assembly.

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

Setting to true will echo the command line statement on the -e --echo

standard output. Default is false.

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

are prompted.

The machine name where the domain administration server -H --host

is running. The default value is localhost.

The HTTP/S port for administration. This is the port to -p --port

which you should point your browser in order to manage the

domain. For example, http://localhost:4848.

The default port number is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

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, including

> the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target where the specified service assembly is deployed. Specify this option only if the service assembly is deployed in a multiserver environment with a Domain Administration Server (DAS). If the service assembly is not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which displays information about the JBI service assembly deployed on the embedded DAS instance. This is the default value.
- domain, which shows information about the JBI service assembly deployed in the administrative domain itself.
 Specify domain only if you are using the cluster profile.

--help

- cluster_name, which shows information about the JBI service assembly on every server instance in the cluster.
- instance_name, which shows information about the JBI service assembly deployed on the named unclustered server instance.

Operands *service_assembly_name*

The name of the JBI service assembly about which you want the detailed information.

Examples EXAMPLE 1 Using the show-jbi-service-assembly command

The following command shows information about a JBI service assembly on the specified server instance.

asadmin> show-jbi-service-assembly --user admin2
--passwordfile passwords.txt --target server1 serviceassemblyname
Command show-jbi-service-assembly executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also list-jbi-service-assemblies(1), deploy-jbi-service-assembly(1)

Name show-jbi-service-engine – shows detailed information about the specified service engine

Synopsis show-jbi-service-engine

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]
[--passwordfile filename] [--help]
[--target target]

[--target target] service_engine_name

Description The show-jbi-service-engine command shows detailed information about the specified

service engine.

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 is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target for which you want to show details of the JBI service engine. Specify this option only if the service engine is deployed in a multiserver environment with a Domain Administration Server (DAS). If the service engine is not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which shows details of the specified service engine on the embedded DAS instance. This is the default value.
- domain, which shows details of the service engine on the administrative domain itself. Specify domain only if you are using the cluster profile.

--help

- *cluster_name*, which shows details of the specified service engine on the cluster.
- instance_name, which shows details of the service engine on the named unclustered server instance.

Operands *service_engine_name*

The name of the JBI service engine about which you want the detailed information.

Examples EXAMPLE 1 Using the show-jbi-service-engine command

The following command shows information about the JBI service engine on the target server.

asadmin> show-jbi-service-engine --user admin2
--passwordfile passwords.txt --target server1 serviceengine1
Command show-jbi-service-engine executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also list-jbi-service-engines(1)

Name show-jbi-shared-library – shows detailed information about a specified shared library

Synopsis show-jbi-shared-library

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help]

[--target target] shared_library_name

Description The show-jbi-shared-library command displays detailed information about a specified

shared library.

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.

Setting to true will echo the command line statement on the -e --echo

standard output. Default is false.

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

are prompted.

The machine name where the domain administration server -H --host

is running. The default value is localhost.

The HTTP/S port for administration. This is the port to -p --port

which you should point your browser in order to manage the

domain. For example, http://localhost:4848.

The default port number is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

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, including

> the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target where the specified shared library is deployed. Specify this option only if the shared library is deployed in a multiserver environment with a Domain Administration Server (DAS). If the shared library is not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which displays information about the JBI shared library deployed on the embedded DAS instance. This is the default value.
- domain, which shows information about the JBI shared library deployed in the administrative domain itself.
 Specify domain only if you are using the cluster profile.

--help

- *cluster_name*, which shows information about the JBI shared library on every server instance in the cluster.
- instance_name, which shows information about the JBI shared library deployed in the named unclustered server instance.

Operands *shared_library_name*

The name of the JBI shared library about which you want the detailed information.

Examples EXAMPLE 1 Using the show-jbi-shared-library command

The following command shows information about a JBI shared library on the specified server instance.

asadmin> show-jbi-shared-library --user admin2
--passwordfile passwords.txt --target server1 sharedlibraryname
Command show-jbi-shared-library executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also list-jbi-shared-libraries(1), install-jbi-shared-library(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 Administration Server page

Equivalent

See Also start-instance(1), stop-instance(1), start-domain(1), stop-domain(1)

Name shut-down-jbi-component – shuts down a service engine or a binding component on the specified target

Synopsis shut-down-jbi-component

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [--force =false] [--target target] component_name

Description The shut-down-jbi-component command shuts down a service engine or a binding component on the specified target. If no target is specified, the component will be shut down on the embedded DAS server.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Setting to true forcibly shuts down the service engine or the binding component. Default is false.

Specifies the target on which you are shutting down the JBI component. Specify this option only if the JBI component is deployed in a multiserver environment with a Domain Administration Server (DAS). If the JBI component is not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

--help

-F -- force

- server, which shuts down the service engine or the binding component on the embedded DAS instance.
 This is the default value.
- domain, which shuts down the service engine or the binding component on the administrative domain itself.
 Specify domain only if you are using the cluster profile.
- cluster_name, which shuts down the service engine or the binding component for every server instance in the cluster.
- instance_name, which shuts down the service engine or the binding component for the named unclustered server instance.

Operands *component_name*

The name of the binding component or the service engine that you want to shut down.

Examples EXAMPLE 1 Using the shut-down-jbi-component command

The following command shuts down a JBI component.

asadmin> shut-down-jbi-component --user admin2
--passwordfile passwords.txt --target NewServer MyWebApp
Command shut-down-jbi-component executed successfully.

Exit Status 0

command executed successfully

1

error in executing the command

See Also start-jbi-component(1), stop-jbi-component(1)

Name shut-down-jbi-service-assembly - shuts down a JBI service assembly on the specified target

Synopsis shut-down-jbi-service-assembly

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user]

[--passwordfile *filename*] [--help]

[--force =false] [--target target] service_assembly_name

Description The shut-down-jbi-service-assembly command shuts down a JBI service assembly on the specified target. If a target is not specified, the command will shut down the JBI service

	assembly on the server, which is the default target.	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Setting to true forcibly shuts down the service assembly. Default is false.

Specifies the target on which you want to shut down the service assembly. Specify this option only if the service assembly is deployed in a multiserver environment with a Domain Administration Server (DAS). If the service assembly is not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

--help

-F -- force

- server, which shuts down the JBI service assembly on the embedded DAS instance. This is the default value.
- domain, which shuts down the JBI service assembly on the administrative domain itself. Specify domain only if you are using the cluster profile.
- *cluster_name*, which shuts down the JBI service assembly on every server instance in the cluster.
- instance_name, which shuts down the JBI service assembly on the named unclustered server instance.

Operands *service_assembly_name*

The name of the JBI service assembly you want to shut down.

Examples EXAMPLE 1 Using the shut-down-jbi-service-assembly command

The following command shuts down a JBI service assembly.

asadmin> shut-down-jbi-server-assembly --user admin2
--passwordfile passwords.txt --target server1 serviceassembly1
Command shut-down-jbi-service-assembly executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also start-jbi-service-assembly(1), stop-jbi-service-assembly(1)

Name start-appsery – starts the domains in the specified domains directory

Synopsis start-appserv [--terse=false] [--echo=false]

[--interactive=true] [--user admin_user]

[--passwordfile passwordfile] [--domaindir install_dir/domains]

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-appsery command functions correctly if every domain is created with --savemasterpassword. 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 <code>install_dir/domains</code> directory is started.
	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on to the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile 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.

```
Examples EXAMPLE1 Using the start—appserv command

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>
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

instance-name

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [--filtertype type=value[type=value]*]

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.

-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
-Iinteractive	If set to true (default), only the required password options are prompted.
-Hhost	The machine name where the domain administration server is running. The default value is localhost.
-pport	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 is 4848.
-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
-uuser	The authorized domain administration server administrative username.
	If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Takes the format type=value, where type can be user or ip.

The name of the application server instance for which you want to enable call flow monitoring.

Examples EXAMPLE 1 Using start-callflow-monitoring

--help

Operands instance-name

---filtertype

asadmin start-callflow-monitoring --passwordfile passwordfile.txt --user admin --host localho Command start-callflow-monitoring executed successfully.

Exit Status 0 command executed successfully

error in executing the command

 $\textbf{See Also} \quad stop\text{-}call flow\text{-}monitoring (1)$

1

Name start-cluster – starts a cluster

Synopsis start-cluster

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --autohadboverride={true|false} ]
cluster name
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide

> The start-cluster command attempts to start all non-running instances in the cluster that are reachable through their node agent. In other words, some instances may not be started if their node agent is not running. If HADB is installed, this command can also start the HADB database associated with a cluster, depending upon the cluster's autohadb setting and whether you override it using this command's autohadboverride 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.

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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help Displays the help text for the command.

--autohadboverride

This option is valid only if the HADB software is installed. The autohadboverride option determines whether to override the cluster's setting for the autohadb option. When the cluster was created, the autohadb option was set to signal whether the HADB database associated with the cluster would be started, stopped, or deleted when the cluster was started, stopped, or deleted. You can override this value using the autohadboverride option. If autohadboverride is set to true, the HADB database is started when the cluster is started. If set to false, the HADB database is not started when the cluster is started. If the autohadboverride option is not set, the default is to use the cluster's autohadb setting.

Operands cluster name

The name of the cluster to be started.

Examples EXAMPLE 1 Using the start-cluster command

The following command starts the cluster named MyCluster.

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

Exit Status 0 command executed successfully

1 error in executing the command

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

Name start-database – starts the Java DB

Synopsis start-database [--dbhost 0.0.0.0] [--dbport 1527] [--dbhome DERBY_INSTALL] [--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.

When the database server starts, or a client connects to it successfully, two types of files are created:

- The derby.log file that contains the database server process log along with its standard output and standard error information.
- The database files that contain your schema (for example, database tables).

Both types of files are created at the location specified by the dbhome option. When -dbhome is not specified, the default is the value of DERBY INSTALL, which defaults to *install-dir/* j avadb. It is important to use the dbhome option when you want to create the database files at a particular location. The start-database command starts the database process, even if it cannot write to the log file.

This command is supported in local mode only.

Options	dbhost	The host name or IP address of the Java DB server process. The default is the IP address 0.0.0.0, which denotes all network interfaces on the host where you run the start-database command.
	dbport	The port number where the Java DB server listens for client connections. This port must be available for the listen socket, otherwise the database server will not start. The default is 1527.
	dbhome	The absolute path to the directory where Java DB and the derby.log files are created. The default is DERBY_INSTALL.
	-eecho	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/javdb/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 domain-dir]
           --user admin_user --passwordfile file_name
           [--terse={true|false}] [ --echo ={true|false}]
           [ --interactive ={true|false}] [ --verbose ={true|false}]
           [ --debug ={true|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.

> You can use the start-domain command to upgrade domains of Application Server 8.x or 9.0 to Application Server 9.1. Use one of the following ways to upgrade your domain:

- Perform an in-place upgrade of the Application Server binaries. When you run start-domain on the domains pointing to the earlier version of Application Server, asadmin invokes the asupgrade command, and the domains are automatically upgraded in-place.
- Perform a side-by-side upgrade of the Application Server binaries. Run start-domain on the domains of your earlier installation. The asupgrade command upgrades the domains to the domains root of the latest Application Server installation. In this scenario, the target directory for the upgrade is defined in the AS DEF DOMAINS PATH in the asenv.conf.

On the Mac OS X platform, 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.

Options --domaindir

The directory where the domain is to be started. If specified, the path must be accessible in the filesystem. If not specified, the domain in the default <code>install_dir/domains</code> directory is started.

-u --user

The authorized domain application server administrative username.

--passwordfile

The file containing the domain application server password associated with the administrative instance. The password is defined in the following form: AS ADMIN PASSWORD=password. Where password is the actual administrator password for the domain.

-t--terse

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.

-e --echo

Setting to true will echo the command line statement on to the standard output. Default is false.

-I --interactive

If set to true (default), only the required 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 domain1
Starting Domain domain1, please wait.
Log redirected to /usr/appserver/domains/domain1/logs/server.log.
Redirecting output to /usr/appserver/domains/domain1/logs/server.log
Domain domain1 started.
Domain [domain1] is running [Sun Java System Application Server 9.1 (build
b50d-beta3)] with its configuration and logs at: [/usr/appserver/domains].
Admin Console is available at [http://localhost:4848].
Use the same port [4848] for "asadmin" commands.
User web applications are available at these URLs:
[http://localhost:8080 https://localhost:8181 ].
Following web-contexts are available:
[/web1 / wstx-services].
Standard JMX Clients (like JConsole) can connect to JMXServiceURL:
[service:jmx:rmi:///jndi/rmi://pdavies.SFBay.Sun.COM:8686/jmxrmi] for domain
management purposes.
Domain listens on at least following ports for connections:
[8080 8181 4848 3700 3820 3920 8686 ].
Domain supports application server clusters and other standalone instances.
```

Where: domain1 is the domain in the /usr/appserver/domains directory.

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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] instance_name

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

This command starts an instance with the instance name you specify.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This is the name of the server instance to start.

Examples EXAMPLE 1 Using start-instance

asadmin> start-instance -- instance_name instance1

Instance instance1 started

Exit Status 0 command executed successfully

1 error in executing the command

Interface Server Instance page **Equivalent**

--help

Operands *instance_name*

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

Name start-jbi-component – starts a service engine or a binding component on the specified target

Synopsis start-jbi-component

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [--target target] component_name

Description The start-jbi-component command starts a service engine or a binding component on the specified target. If no target is specified, the component will be started on the Domain Administration Server (DAS).

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin

--passwordfile

The -- passwordfile option specifies the name, including the full path, 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.

login command, then you need not specify the --user option on subsequent operations to this particular domain. For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target on which you are starting the JBI component. Specify this option only if the JBI component is deployed in a multiserver environment with a Domain Administration Server (DAS). If the JBI component is not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which starts the service engine or the binding component on the embedded DAS instance. This is the default value.
- domain, which starts the service engine or the binding component on the administrative domain itself. Specify domain only if you are using the cluster profile.

--help

--target

- cluster_name, which starts the service engine or the binding component for every server instance in the cluster.
- instance_name, which starts the service engine or the binding component for the named unclustered server instance.

Operands component_name

The name of the binding component or the service engine that you want to start.

Examples EXAMPLE 1 Using the start-jbi-component command

The following command starts a JBI component.

```
asadmin> start-jbi-component --user admin2
--passwordfile passwords.txt --target NewServer MyWebApp
Command start-jbi-component executed successfully.
```

Exit Status 0 command executed successfully

1 error in executing the command

See Also install-jbi-component(1), list-jbi-binding-components(1), list-jbi-service-engines(1), stop-jbi-component(1), shut-down-jbi-component(1), uninstall-jbi-component(1)

Name start-jbi-service-assembly – starts a service assembly on the specified target

Synopsis start-jbi-service-assembly

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help]

[--target target]

service_assembly_name

Description The start-jbi-service-assembly command starts a JBI service assembly on the JBI specified target. If a target is not specified, the command will start the JBI service assembly on the server, which is the default target.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target on which you want to start the service assembly. Specify this option only if the service assembly is deployed in a multiserver environment with a Domain Administration Server (DAS). If the service assembly is not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which starts the JBI service assembly on the embedded DAS instance. This is the default value.
- domain, which starts the JBI service assembly on the administrative domain itself. Specify domain only if you are using the cluster profile.

--help

--target

- cluster_name, which starts the JBI service assembly on every server instance in the cluster.
- instance_name, which starts the JBI service assembly on the named unclustered server instance.

Operands *service_assembly_name*

The name of the JBI service assembly.

Examples EXAMPLE 1 Using the start-jbi-service-assembly command

The following command starts a JBI service assembly.

asadmin> start-jbi-server-assembly --user admin2

--passwordfile passwords.txt --target server1 serviceassembly1
Command start-jbi-service-assembly executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also install-jbi-component(1), start-jbi-component(1), list-jbi-binding-components(1),

list-jbi-service-engines(1), stop-jbi-component(1), shut-down-jbi-component(1),

uninstall-jbi-component(1)

Name start-node-agent – starts a node agent

Synopsis start-node-agent [--user *user*]

```
[--passwordfile passwordfile] [--secure={true|false}]
[ --terse={true|false} ] [ --echo={true|false} ]
[ --interactive={true|false} ] [ --verbose={true|false} ]
[ --agentdir nodeagent_path] [--startinstances={true|false}]
[ --syncinstances={true|false} ] [nodeagent_name]
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> Use the start-node-agent command start a node agent. The command will return control to the user before instances are actually started. The list-instances command can be executed to see if they have actually started. This command may take a while to execute since the node agent may need to create and start a number of server instances.

This command is supported in local mode only.

Options

-u --user

The authorized domain administration server administrative username.

--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 administration 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 administration 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 administration 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

-s --secure

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

-t --terse

Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.

-e --echo

Setting to true will echo the command line statement on the standard output. Default is false.

-T -- interactive

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

-h --help

Displays the help text for the command.

--verbose

By default this flag is set to false. If set to true, a console window is opened for the node agent and for every server instance a node agent manages. On Windows, press Ctrl-Break in the console to print a thread dump. On UNIX, press CTRL-Backslash in the console to print a thread dump. The node agent thread dump goes to its console. The server instance thread dump goes to the instance log file.

--agentdir

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

--startinstances

If set to true, all server instances that are not currently running are started. If set to false, instances are not started. If the option is omitted, it defaults to the value of the node agent's start-servers-in-startup attribute, located in the domain.xml file.

--syncinstances

If set to true, forcibly synchronizes the cache repositories of *all* server instances with the central repository of the DAS. The synchronization occurs when the node agent is started. For more information, see "Synchronizing Node Agents and the Domain Administration Server" in *Sun Java System Application Server 9.1 High Availability Administration Guide*. Default is false.

Operands *nodeagent_name*

The name of the node agent to be started.

Examples EXAMPLE 1 Using the start-node-agent command

asadmin> start-node-agent --user admin
--passwordfile passwordfile nodeagent1

Nodeagent1 started.

The node agent nodeagent1 is started in the default <code>install_dir/nodeagents</code> directory.

Exit Status 0 command executed successfully

1 error in executing the command

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

Sun Java System Application Server 9.1 High Availability Administration Guide

Name stop-appsery – stops the domains in the specified domains directory

Synopsis stop-appserv [--domaindir *install dir*/domains]

[--terse=false] [--echo=false]

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.

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={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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.

-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
-Iinteractive	If set to true (default), only the required password options are prompted.
-Hhost	The machine name where the domain administration server is running. The default value is localhost.
-pport	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.
	TTI 1 C 1

The default port number is 4848.

-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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

The name of the application server instance for which you want to diable call flow monitoring.

Examples EXAMPLE 1 Using stop-callflow-monitoring

--help

Operands instance-name

1

asadmin **stop-callflow-monitoring --passwordfile passwordfile.txt --user admin --host localhost --p**Command stop-callflow-monitoring executed successfully.

Exit Status 0 command executed successfully

error in executing the command

See Also start-callflow-monitoring(1)

Name stop-cluster – stops a cluster

Synopsis stop-cluster

```
[--terse={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
[ --autohadboverride={true|false} ] cluster name
```

Description Note – This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> The stop-cluster command attempts to stop all running instances in the cluster that are reachable through their node agent. In other words, some instances may not be stopped if their node agent is not running. If HADB is installed, this command can also stop the HADB database associated with a cluster, depending upon the cluster's autohadb setting and whether you override it using this command's autohadboverride 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 is 4848.

-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, including the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

--help

Displays the help text for the command.

--autohadboverride

This option is valid only if the HADB software is installed. The autohadboverride option determines whether to override the cluster's setting for the autohadb option. When the cluster was created, the autohadb option was set to signal whether the HADB database associated with the cluster would be started, stopped, or deleted when the cluster was started, stopped, or deleted. You can override this value using the autohadboverride option. If autohadboverride is set to true, the HADB database is stopped when the cluster is stopped. If set to false, the HADB database is not stopped when the cluster is stopped. If the autohadboverride option is not set, the default is to use the cluster's autohadb setting.

Operands cluster name

The name of the cluster to be started.

Examples EXAMPLE 1 Using the stop-cluster command

The following command stops the cluster named MyCluster.

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

Exit Status 0 command executed successfully
1 error in executing the command
See Also start-cluster(1), create-cluster(1), list-clusters(1), delete-cluster(1)
```

Name stop-database – stops Java DB

Synopsis stop-database [--dbhost 0.0.0.0] [--dbport 1527]

Description The stop-database command stops 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.

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 value of DERBY INSTALL, which defaults to *install-dir*/javadb.

> 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 [--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] instance name

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> Use the stop-instance to stop the instance with the instance name specified. The stop-instance can be run both locally and remotely. The named instance must already exist within the given domain; and the instance must be running.

		8
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser

option on subsequent operations to this particular domain.

The -- passwordfile option specifies the name, including the full path, of a file containing the password entries in a

--passwordfile

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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This is the name of the server instance to stop.

Examples EXAMPLE 1 Using stop-instance in local mode

asadmin> stop-instance --local --domain domain1 server1

Instance server1 stopped

--help

Operands *instance_name*

Where: the server1 instance associated with the domain1 domain is stopped locally.

EXAMPLE 2 Using stop-instance in remote mode

asadmin> stop-instance --user admin --password bluestar --host localhost --port 4848 server1 Instance server1 stopped

Where: the server1 instance associated with the named user, password, host and port is deleted from the remote machine.

Exit Status 0 command executed successfully

1 error in executing the command

Interface Equivalent

Server Instance page

- Coo Ma

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

Name stop-jbi-component – stops a service engine or a binding component on the specified target

Synopsis stop-jbi-component

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [--target target] component_name

Description The stop-jbi-component command stops a service engine or a binding component on the specified target. If no target is specified, the component will be stopped on the embedded DAS server.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target on which you are stopping the JBI component. Specify this option only if the JBI component is deployed in a multiserver environment with a Domain Administration Server (DAS). If the JBI component is not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which stops the service engine or the binding component on the embedded DAS instance. This is the default value.
- domain, which stops the service engine or the binding component on the administrative domain itself. Specify domain only if you are using the cluster profile.

--help

--target

- cluster_name, which stops the service engine or the binding component for every server instance in the cluster.
- instance_name, which stops the service engine or the binding component for the named unclustered server instance.

Operands component_name

The name of the binding component or the service engine that you want to stop.

Examples EXAMPLE 1 Using the stop-jbi-component command

The following command stops a JBI component.

asadmin> stop-jbi-component --user admin2

--passwordfile passwords.txt --target NewServer MyWebApp

Command stop-jbi-component executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also start-jbi-component(1), shut-down-jbi-component(1), uninstall-jbi-component(1)

Name stop-jbi-service-assembly – stops a service assembly on the specified target

Synopsis stop-jbi-service-assembly

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

[--target target] service_assembly_name

Description The stop-jbi-service-assembly command stops a JBI service assembly on the specified target. If a target is not specified, the command will stop the JBI service assembly on the server, which is the default target.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.

If set to true, uses SSL/TLS to communicate with the domain -s --secure

administration server.

The authorized domain administration server -u --user

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, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Specifies the target on which you want to stop the service assembly. Specify this option only if the service assembly is deployed in a multiserver environment with a Domain Administration Server (DAS). If the service assembly is not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which stops the JBI service assembly on the embedded DAS instance. This is the default value.
- domain, which stops the JBI service assembly on the administrative domain itself. Specify domain only if you are using the cluster profile.

--help

--target

- *cluster_name*, which stops the JBI service assembly on every server instance in the cluster.
- instance_name, which stops the JBI service assembly on the named unclustered server instance.

Operands *service_assembly_name*

The name of the JBI service assembly you want to stop.

Examples EXAMPLE 1 Using the stop-jbi-service-assembly command

The following command stops a JBI service assembly.

asadmin> stop-jbi-server-assembly --user admin2

--passwordfile passwords.txt --target server1 componentname
Command stop-jbi-service-assembly executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also start-jbi-service-assembly(1)

Name stop-node-agent – stops a node agent

Synopsis stop-node-agent [--agentdir nodeagent path]

[--terse=false] [--echo=false]

[--interactive=true] [nodeagent_name]

Description Note - This command is available only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. For information about profiles, see "Usage Profiles" in Sun Java System Application Server 9.1 Administration Guide.

> The local stop-node-agent command is used to stop a node agent. If the agent directory is not specified, the node agent in the default install_dir/nodeagents directory is stopped. The stop-node-agent commands stops all managed server instances of the node agent.

This command is supported in local mode only.

Options --agentdir Like a Domain Administration Server (DAS), each node

agent resides in a top level directory named

agentdir/nodeagent_name. If specified, the path must be accessible in the filesystem. If not specified, defaults to the

install dir/nodeagents directory.

-t --terse Indicates that any output data must be very concise, typically

avoiding human-friendly sentences and favoring

well-formatted data for consumption by a script. Default is

false.

Setting to true will echo the command line statement on to -e --echo

the standard output. Default is false.

-I -- Interactive If set to true (default), only the required options are

prompted.

Operands nodeagent_name The name of the node agent to stop.

Examples EXAMPLE 1 Using stop-node-agent

asadmin> stop-node-agent nodeagent1

The node agent, nodeagent1, located in default *install_dir*/nodeagents is stopped.

Exit Status 0 command executed successfully

> 1 error in executing the command

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

Name undeploy – removes a deployed component

Synopsis undeploy

[--terse={true|false}][--echo={true|false}]
[--interactive={true|false}] [--host host]
[--port port] [--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.

	11	7.
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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.

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

--help

--droptables

--cascade

--target

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

This option is valid only in domains that are configured to support clusters, such as domains that are created with the cluster profile or the enterprise profile. 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 undeploy-jbi-service-assembly – undeploys a service assembly on the specified target

Synopsis undeploy-jbi-service-assembly

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [--force =false] [--keeparchive=false]

[--target target] service_assembly_name

Description The undeploy-jbi-service-assembly command undeploys a service assembly on the specified target. If the target is not specified, the command will be executed on the server

	instance.	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including

the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Setting to true forcibly undeploys the service assembly. Default is false.

Setting to true retains the service assembly that is stored in the Domain Administration Server (DAS) repository. The service assembly is retained even if the service assembly is undeployed from all servers in the JBI environment. Setting this option to true enables you to re-deploy the service assembly from the DAS repository instead of re-deploying the service assembly from an archive file.

--help

-F -- force

--keeparchive

Setting to false deletes the service assembly from the DAS repository when the service assembly is no longer deployed on any server in the IBI environment.

Default is false.

--target

Specifies the target on which you are undeploying the service assembly. Specify this option only if the service assembly is deployed in a multiserver environment with a Domain Administration Server (DAS). If the service assembly is not deployed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which undeploys the JBI service assembly on the embedded DAS instance. This is the default value.
- domain, which undeploys the JBI service assembly on the administrative domain itself. Specify domain only if you are using the cluster profile.
- *cluster_name*, which undeploys the JBI service assembly on every server instance in the cluster.
- instance_name, which undeploys the JBI service assembly on the named unclustered server instance.

Operands *service_assembly_name*

The name of the JBI service assembly you want to undeploy.

Examples EXAMPLE 1 Using the undeploy-jbi-service-assembly command

The following command undeploys a JBI service assembly.

asadmin> undeploy-jbi-service-assembly --user admin2
--passwordfile passwords.txt --target server1 service_assembly_name
Command undeploy-jbi-service-assembly executed successfully.

Exit Status 0

command executed successfully

1

error in executing the command

See Also deploy-jbi-service-assembly(1), list-jbi-service-assemblies(1), show-jbi-service-assembly(1)

Name unfreeze-transaction-service – resumes all suspended transactions

```
Synopsis unfreeze-transaction-service
```

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--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.

	omy.	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.

--passwordfile

The -- passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

--help 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

Examples EXAMPLE 1 Using unfreeze-transaction-service

asadmin> unfreeze-transaction-service --user admin --passwordfile password.txt --target server

Command unfreeze-transaction-service executed successfully

Exit Status 0 command executed successfully

1 error in executing the command

See Also freeze-transaction-service(1), rollback-transaction(1)

Name uninstall-jbi-component – uninstalls a service engine or binding component on the specified target

Synopsis uninstall-jbi-component

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile filename] [--help] [--force =false] [--keeparchive=false] [--target target] component_name

Description The uninstall-jbi-component command uninstalls a service engine or binding component on the specified target. If no target is specified, the component on the embedded Domain Administration Server (DAS) will be uninstalled.

Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Setting to true forcibly uninstalls the service engine or the binding component. Default is false.

Setting to true retains the JBI component that is stored in the DAS repository. The JBI component is retained even if the JBI component is uninstalled from all servers in the JBI environment. Setting this option to true enables you to reinstall the JBI component from the DAS repository instead of reinstalling the JBI component from an archive file.

--help

-F -- force

--keeparchive

Setting to false deletes the JBI component from the DAS repository when the JBI component is no longer installed on any server in the JBI environment.

Default is false.

--target

Specifies the target on which you are uninstalling the JBI component. Specify this option only if the JBI component is installed in a multiserver environment with a DAS. If the JBI component is not installed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which uninstalls the JBI component on the embedded DAS instance. This is the default value.
- domain, which uninstalls the JBI component on the administrative domain itself. Specify domain only if you are using the cluster profile.
- *cluster_name*, which uninstalls the JBI component on every server instance in the cluster.
- instance_name, which uninstalls the JBI component on the named unclustered server instance.

Operands component name

The name of the JBI component you want to uninstall.

Examples EXAMPLE 1 Using the uninstall-jbi-component command

The following command uninstalls a JBI component.

asadmin> uninstall-jbi-component --user admin2
--passwordfile passwords.txt --target server1 component_name
Command uninstall-jbi-component executed successfully.

Exit Status 0

command executed successfully

1

error in executing the command

See Also install-jbi-component(1)

Name uninstall-jbi-shared-library – uninstalls a shared library on the specified target

Synopsis uninstall-jbi-shared-library

--passwordfile

[--terse={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

[--keeparchive =false]

[--target target] shared_library_name

Description The uninstall-jbi-shared-library command uninstalls a shared library on the specified target. If no target is specified, the shared library on the embedded Domain Administration Server (DAS) is uninstalled.

	server (D/13) is diffilstaticd.	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.

uppercase letters.

The --passwordfile option specifies the name, including the full path, 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

For example, to specify the domain administration server password, use an entry with the following format: 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

Setting to true retains the shared library that is stored in the DAS repository. The shared library is retained even if the shared library is uninstalled from all servers in the JBI environment. Setting this option to true enables you to reinstall the shared library from the DAS repository instead of reinstalling the shared library from an archive file.

Setting to false deletes the shared library from the DAS repository when the shared library is no longer installed on any server in the JBI environment.

Default is false.

--help

--keeparchive

--target

Specifies the target on which you are uninstalling the JBI shared library. Specify this option only if the shared library is installed in a multiserver environment with a Domain Administration Server (DAS). If the shared library is not installed in a multiserver environment with a DAS, this option is ignored. Valid values are:

- server, which uninstalls the JBI shared library on the embedded DAS instance. This is the default value.
- domain, which uninstalls the JBI shared library on the administrative domain itself. Specify domain only if you are using the cluster profile.
- *cluster_name*, which uninstalls the JBI shared library on every server instance in the cluster.
- instance_name, which uninstalls the JBI shared library on the named unclustered server instance.

Operands *shared_library_name*

The name of the JBI shared library you want to uninstall.

Examples EXAMPLE 1 Using the uninstall-jbi-shared-library command

The following command uninstalls a JBI shared library.

asadmin> uninstall-jbi-shared-library --user admin2
--passwordfile passwords.txt --target server1 filepath
Command uninstall-jbi-shared-library executed successfully.

Exit Status 0 co

command executed successfully

1 error in executing the command

See Also install-jbi-shared-library(1), list-jbi-shared-libraries(1), show-jbi-shared-library(1)

706

Name unpublish-from-registry – unpublishes the web service artifacts from the registries

Synopsis unpublish-from-registry --registryjndinames registrynames

--webservicename qualified_webservice_name
[--terse={true|false}][--echo={true|false}]

[--interactive={true|false}] [--host host]
[--port port] [--secure| -s] [--user admin_user]

[--passwordfile filename] [--help]

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

-t -- terse Indicates that any output data must be very concise, typically

avoiding human-friendly sentences and favoring

well-formatted data for consumption by a script. Default is

false.

-e --echo Setting to true will echo the 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 is 4848.

-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, including

the full path, 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.

The default value for AS ADMIN MASTERPASSWORD is changeit.

Displays the help text for the command.

--help

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 [name [name]*] **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 name 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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
    --poolname connector_connection_pool_name
[ --addprincipals principal_name1[, principal_name1]*| --addusergroups user_group1[,user_group2] ]
[ --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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.

--passwordfile

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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This option is deprecated.

Specifies the name of the connector connection pool to which the security map that is to be updated or created belongs.

--help

--target

--poolname

Specifies a comma-separated list of EIS-specific principals to --addprincipals be added. Use either the --addprincipals or -- addusergroups options, but not both at the same time. Specifies a comma-separated list of EIS user groups to be --addusergroups 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. Specifies a comma-separated list of EIS user groups to be --removeusergroups removed. Specifies the EIS username. --mappedusername **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 connector Command update-connector-security-map executed successfully Fxit 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={true|false}][--echo={true|false}] [--interactive={true|false}] [--host host] [--port port] [--secure| -s] [--user admin_user] [--passwordfile *filename*] [--help] [--groups user_groups[:user_groups]*]

[--authrealmname authrealm_name] [--target target]

username

-u --user

--passwordfile

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 (:)

	password and groups. Manufic groups can be effected by separating them, with a colon (.)	
Options	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.

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

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.

The -- passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This is the name of the group to which the file user belongs.

This is the file where the user may have different stores for file auth realm.

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.

- --help
- --groups
- --authrealmname
- --target

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--secure| -s ] [ --user admin_user]
[--passwordfile filename] [--help]
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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

This is the name of the password as it appears in domain.xml.

Examples EXAMPLE 1 Using update-password-alias

--help

Operands -aliasname

asadmin> update-password-alias --user admin --passwordfile /home/password.txt jmspassword-ali 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

 $\textbf{See Also} \quad \text{delete-password-alias} (1), \text{list-password-aliases} (1), \text{create-password-alias} (1)$

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 <code>install_dir/domains</code>.

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={true|false}][ --echo={true|false} ]
[ --interactive={true|false} ] [ --host host]
[--port port] [--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	-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
	-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
	-Iinteractive	If set to true (default), only the required password options are prompted.
	-Hhost	The machine name where the domain administration server is running. The default value is localhost.
	-pport	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 is 4848.
	-ssecure	If set to true, uses SSL/TLS to communicate with the domain administration server.
	-uuser	The authorized domain administration server administrative username.
		If you have authenticated to a domain using the asadmin login command, then you need not specify theuser option on subsequent operations to this particular domain.
	passwordfile	Thepasswordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

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

--help

--verbose

Version = Sun Java System Application Server 9.1 Command version executed successfully.

Exit Status 0 command executed successfully

1 error in executing the command

See Also help(1)

REFERENCE

Application Server 9.1 Section 1M: Utility Commands

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

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

Attributes See attributes(5) for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Interface Stability	Unstable

See Also package-appclient(1M), asadmin(1M)

Name asadmin – utility for performing administrative tasks for the Sun Java System Application Server

Synopsis 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:

-tterse	Indicates that any output data must be very concise, typically avoiding human-friendly sentences and favoring well-formatted data for consumption by a script. Default is false.
-eecho	Setting to true will echo the command line statement on the standard output. Default is false.
-Iinteractive	If set to true (default), only the required password options are prompted.
-Hhost	The machine name where the domain administration server is running. The default value is localhost.
-pport	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 is 4848.
-ssecure	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.

The --passwordfile option specifies the name, including the full path, 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.

The default value for AS_ADMIN_MASTERPASSWORD is changeit.

Displays the help text for the command.

--passwordfile

--help

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 See attributes(5) for descriptions of the following 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.
iaiyets	COMPTICE	complies an java source code.

assembles the EJB JAR module. jar

assembles the WAR file in sample_dir/assemble/war war

assembles the EAR file in sample_dir/assemble/ear ear

(default) compiles all sources, builds stubs and skeletons; core

> 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.

creates Java docs in *sample_dir/* javadocs 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.

removes appname/build/ and appname/assemble/ and clean

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-files=true
           [ --append -logs] [operands]
```

Description Use the asmigrate utility to analyze your J2EE application and translate vendor specific settings to SunJavaTM 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	

	Tollicat Web Server 4.1.12	
Options	-hhelp	displays the arguments for launching the MigrationTool.
	-vversion	displays the version of the MigrationTool.
	-uui	invokes the tool in user interface mode.
	-ccommandline	invokes the tool in command-line mode.
	-qquiet	launches the tool in quiet mode.
	-ddebug	launches the tool in debug mode.
	-ssourcedirectory	identifes the directory where the source code to migrate or scan is present.

-S --sourceserver

identifies the source application server of the applications to be migrated. Possible servers include the following:

- 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
- as 70: Sun ONE Application Server 7.0
- ws40: WebSphere Application Server 4.0
- ws50: WebSphere Application Server 5.x
- ri 13: Java
T $\bar{\mathbf{M}}^{\text{TM}}$ 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.

-f --file-filter

 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.

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 a supgrade – migrates the configuration of a previously installed Sun Java System Application Server

```
Synopsis asupgrade [--console] [ --version ]
          [ --help ] [ --source applicationserver 8.x_installation]
          [--target applicationserver 9.1 installation]
          [--adminuser admin_user] [--passwordfile path_to_password_file]
```

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 domain's 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

Exit Status 0

command executed successfully

1

error in executing the command

See Also asmigrate(1m)

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 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

--userdir

displays the arguments for launching the deploytool.

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.

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

--verbose

Examples EXAMPLE 1 Using deploytool

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

Where -- userdir specifies the destination directory, and -config diridentifies the configuration directory.

See Also verifier(1M)

Name jspc – precompiles JSP source files into servlets

Synopsis jspc [options] jsp_files

[options] -webapp dir jspc

Description Use the j spc 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.

Enables verbose mode. - V

-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.

-1 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.

Generates separate write () calls for each HTML line and mapped

> 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 j spc 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 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/img/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 your Client Stub.jar

Attributes See attributes(5) for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Interface Stability	Unstable

See Also appclient(1M)

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.

Specifies the location of the user-specified files. -classpath *path*

-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 schemal.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 schemal.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 schemal.xsd

 $\begin{array}{ll} \textbf{EXAMPLE 3} & \textbf{Using schemagen to generate schema files and specify the location of the generated class files} & (Continued) \end{array}$

This example shows how to generate the schema file with a specified location for the generated class files.

See Also xjc(1M)

Name updatedool - dynamically installs any updated components

Synopsis updatetool [gui | tray | scheduler | all | help]

Description This command launches the Update Center utility. Use the Update Center to install additional

modules and/or update existing modules with the latest download version. The Update Center displays the modules that are available for installation or update. Based on the user settings, the utility downloads the selected module distribution files, performs their

installation, and updates the local registry of the installed modules.

Operands gui launches the Update Center graphical interface.

tray Windows only; launches the Update Center graphical interface and starts

the tray icon.

scheduler launches the Update Center graphical interface with the schedule tab

active.

all launches the Update Center graphical interface and starts the tray icon

process and scheduler.

help displays a usage message.

Examples EXAMPLE 1 Sending output to the screen:

updatetool all

Exit Status 0 command executed successfully

1 error in executing the command

See Also asadmin(1M)

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 <code>jar_filename.xml</code> and <code>jar_filename.txt</code>

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.
name of the ear/war/jar/rar file to perform static verification on. The results of verification are placed in two files <code>jar_filename.xml</code> and <code>jar_filename.txt</code> in the destination directory.	

Operands *jar_filename*

--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 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, ws compile 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.

> where to place the generated output files. -d directory

-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.

generates the debugging information. - q

-gen-gen:client generates the client-side artifacts.

generates the server-side artifacts and the WSDL file. If you -gen:server

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.

writes the mapping file to the specified file. -mapping *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.

keeps the generated files. -keep

-nd *directory* directory for the non-class generated files are stored.

-0 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 features.

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

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.

enable unwrapping of document/literal wrapper elements in unwrap

WSI mode.

allow generation of one-way operations. useonewayoperations

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"</pre>

targetNamespace="http://echoservice.org/wsdl"

typeNamespace="http://echoservice.org/types"

packageName="stub tie generator test">

<interface name="stub tie generator test.CollectionIF"</pre>

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 ws compile 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 ws compile 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 temporary files. -keep

-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.

generates code for the specified JAX-RPC SI version. -source 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 that implements the interface. The web.xml file is tghe deployment descriptor of a web component.

File

jaxrpc-ri.xml 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 opposite direction, from schema types to Java types. In this case, the generated schema types are taken from the package that the type comes from.

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

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

```
<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.

specifies a catalog file to resolve external entity references. -catalog

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.

specifies the target package, overriding any WSDL and - p

> 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.

output messages about what the compiler is doing. -verbose

-version prints version information.

The value of the @WebService.wsdlLocation and -wsdllocation URI

> @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 x j c 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.

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.

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.

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.

Specify a target package to override any binding customization for package name and the default package

name algorithm defined in the specification.

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.

_	. •	
()	ptions	

-extension

-b file

-d directory

-p package

-httpproxy *proxy*

Specify where to find client application class files used by the -classpath arg <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. Supress the generation of package level annotations into -npa **/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. Display a brief summary of the compiler switches. -help -version Display the compiler version information. -Xlocator Enable source location support for generated code.. Generate accessor methods with the synchronized -Xsync-methods keyword. -mark-generated Mark the generated code with the -@javax.annotation.Generated annotation.

Compiler Restrictions

Extensions

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.

 $\hbox{\bf EXAMPLE 3} \quad \hbox{\bf Using xjc to compile schema and put generated Java sources in specified package under specified directory } \\$

```
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 x j c 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.

 $\textbf{EXAMPLE 5} \quad \text{Using xjc to compile schema in selected directory and put generated Java sources in specified directory } \\$

```
xjc -d gen-src schemadir
```

EXAMPLE 5 Using x j c to compile schema in selected directory and put generated Java sources in specified directory (*Continued*)

Compile all schema files in the schemadir directory. Generated Java sources will be placed in the gen-src directory.

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)

REFERENCE

Application Server 9.1 Section 5ASC:
Application Server Concepts

Name application – server-side Java applications and Web services

Description The Java EE platform enables applications to access systems that are outside of the application

server. Applications connect to these systems through resources. The Application Server infrastructure supports the deployment of many types of distributed applications and is an ideal foundation for building applications based on Service Oriented Architectures (SOA). SOA is a design methodology aimed at maximizing the reuse of application services. These

features enable you to run scalable and highly available J2EE applications.

See Also create-application-ref(1)

Name cluster – a group of server instances sharing the same set of applications, resources, and configuration information

Description A cluster is a group of application server instances that work together as one logical entity.

Each Application Server instance in the cluster has the same configuration and the same applications deployed to it. Horizontal scaling is achieved by adding Application Server instances to a cluster, thereby increasing the capacity of the system. It is possible to add Application Server instances to a cluster without disrupting service. The HTTP, RMI/IIOP, and JMS load balancing systems distribute requests to healthy Application Server instances in

See Also create-cluster(1)

the cluster.

Name configuration – Application server instances, deployed applications, resources, domains each have their own configurations

Description You can change the configurations for JMS resources, HTTP connectors, clusters, load balancers. Use the the asadmin commands to configure these elements.

See Also configure-lb-weight(1)

Name domain – Domains have their own configurations.

Description A domain provides a common authentication and administration point for a collection of

zero or more server instances. The administration domain encompasses several manageable resources, including instances, clusters, and their individual resources. A manageable

resource, such as a server instance, may belong to only one domain.

Name dotted-names – syntax for using periods to separate names.

Description Dotted name attributes can be used to address the MBean and its attributes.

Name instance – an Application Server instance has its own Java EE configuration, Java EE resources, application deployment areas, and server configuration settings.

Description The Application Server creates one application server instance, called server at the time of installation. You can delete the server instance and create a new instance with a different name.

> For many users, one application server instance meets their needs. However, depending upon your environment, you might want to create additional application server instances. For example, in a development environment you can use different application server instances to test different Application Server configurations, or to compare and test different application deployments. Because you can easily add or delete an application server instance, you can use them to create temporary "sandbox" areas to experiment with while developing.

See Also create-instance(1)

Name loadbalancer – Provide HTTP session failover.

Description Application Server provides high availability of HTTP requests and session data (both HTTP session data and stateful session bean data). J2EE applications typically have significant amounts of session state data. A web shopping cart is the classic example of a session state. Also, an application can cache frequently-needed data in the session object. In fact, almost all applications with significant user interactions need to maintain session state. Both HTTP sessions and stateful session beans (SFSBs) have session state data.

Name logging – logging application server events

Description

The Application Server uses the Java 2 platform Logging API specified in JSR 047. Application Server logging messages are recorded in the server log, normally found at domain-dir/logs/server.log.

The domain-dir/logs directory contains two other kinds of logs in addition to the server log. In the access subdirectory are the HTTP Service access logs, and in the tx subdirectory are the Transaction Service logs. For information about these logs, consult the Admin Console online help and Configuring Transactions. The components of the Application Server generate logging output. Application components can also generate logging output.

Application components may use the Apache Commons Logging Library to log messages. The platform standard JSR 047 API, however, is recommended for better log configuration.

Name monitoring – To observe the runtime state of various components and services deployed in a server instance of the Application Server.

Description The information on the state of runtime components and processes makes it possible to identify performance bottlenecks for tuning purposes, aid capacity planning, predict failures, do root cause analysis in case of failures, and ensure that everything is functioning as expected.

Name node-agent – manages and facilitates remote server instances.

Description You can use a node agent for creating, starting, stopping, and deleting a server instance. Use

the command line interface (CLI) commands to set up node agents.

See Also create-node-agent(1)

Name passwords – securing and managing application server

Description An application server administrator manages one or more domains, each of which can have

distinct administrative credentials. By managing a domain an administrator effectively manages various resources like server instances, server clusters, libraries etc. that are required

by the enterprise Java applications.

Name resources – Provide connectivity to various types of EIS .

Description Application Server provides support JDBC, JMS, and JNDI resources.

Name security – secure and administer application server applications

Description Security is about protecting data: how to prevent unauthorized access or damage to it in

storage or transit. The Application Server; has a dynamic, extensible security architecture based on the J2EE standard. Built in security features include cryptography, authentication and authorization, and public key infrastructure. The Application Server is built on the Java security model, which uses a sandbox where applications can run safely, without potential risk

to systems or users.

Index

A	asadmin, 726
a group of server instances sharing the same set of applications, resources, and configuration information., 769	asant, 729 asmigrate, 732 asupgrade, 736
add an existing cluster or server instance to an existing load balancer configuration or load balancer, 100	automates migration of J2EE applications from other J2EE platforms to Sun Java System Application Server, 732
add-resources, 14 adds a connection pool with the specified connection pool name, 63	Server, 732
adds a lifecycle module, 148 adds a new HTTP listener socket, 105 adds a new unbound node agent to a domain, 170 adds an audit-module, 52 adds an IIOP listener, 109 adds the administered object with the specified JNDI name, 46	B backup-domain, 20 brings down the administration server and associated instances, 641 browses and queries the JNDI tree, 538
adds the named authentication realm, 55 allows you to execute multiple commands while preserving environment settings and remaining in the asadmin utility, 598 an Application Server instance has its own Java EE configuration, Java EE resources, application deployment areas, and server configuration settings., 773	capture-schema, 738 change-master-password, 22, 23 changes the master password, 22, 23 checks to see if the JMS service is up and running, 438 clear-ha-store, 25 cluster, 769
appclient, 724 application, 768 Application server instances, deployed applications, resources, domains each have their own configurations., 770 applies load balancer configuration changes to the load balancer, 18 apply-http-lb-changes, 18	configuration, 770 configure-ha-cluster, 28 configure-ha-persistence, 33 configure-lb-weight, 37 configure-webservice-management, 40 configures an existing cluster to be highly available, 28 configures the starting of a DAS or node agent on an unattended boot, 189

connectivity., 779	create-ssl, 191
connector module, 183	create-system-properties, 195
copies an existing configuration to create a new	create-transformation-rule, 200
configuration, 43	create-virtual-server, 203
copy-config, 43	create-jms-host, 132
create-admin-object, 46	creates a cluster, 58
create-application-ref, 49	creates a configuration for the load balancer, 96
create-audit-module, 52	creates a custom resource, 73
create-auth-realm, 55	creates a domain with the given name, 76
create-cluster, 58	creates a health-checker for a specified load balancer
create-connector-connection-pool, 63	configuration, 88
create-connector-resource, 67	creates a JavaMail session resource, 117
create-connector-security-map, 70	creates a JDBC resource with the specified JNDI
create-custom-resource, 73	name, 126
create-domain, 76	creates a JMS host, 132
create-file-user, 82	creates a JMS physical destination, 129
create-ha-store, 85	creates a JMS resource, 135
create-http-health-checker, 88	creates a list of file users, 492
create-http-lb, 91	creates a load balancer, 91
create-http-lb-config, 96	creates a new file user, 82
create-http-lb-ref, 100	_
create-http-listener, 105	creates a new management rule, 151 creates a node agent, 167
create-iiop-listener, 109	•
create-instance, 112	creates a password alias, 173
create-javamail-resource, 117	creates a reference to a resource, 186
create-jdbc-connection-pool, 121	creates a reference to an application, 49
create-jdbc-resource, 126	creates a schema file for each namespace referenced in
create-jms-resource, 135	your Java classes, 746
create-jmsdest, 129	creates a security map for the specified connector
create-jndi-resource, 141	connection pool, 70
create-jvm-options, 145	creates an instance, 112
create-lifecycle-module, 148	creates and configures the SSL element in the selected
create-management-rule, 151	HTTP listener, IIOP listener, or IIOP service, 191
create-mbean, 159	creates and registers a custom MBean, 159
create-message-security-provider command, 163	creates or modifies a security map for the specified
create-node-agent, 167	connector connection pool, 710
create-node-agent-config, 170	creates tables in the HADB that are used by HA the
create-password-alias, 173	cluster, 85
create-persistence-resource,	creates the JVM options from the Java configuration or
create-persistence-resource, 176	profiler elements, 145
create-profiler, 180	creates the named virtual server, 203
create-resource-adapter-config command, 183	creates the profiler element, 180
create-resource-ref, 186	creates transformation rule for a deployed web
create-service, 189	service, 200

υ	deletes a health-checker for a specified load balancer
delete, 222	configuration, 243
delete-admin-object, 210	deletes a load balancer, 246
delete-application-ref, 213	deletes a load balancer configuration, 248
delete-auth-realm, 219	deletes a password alias, 302
delete-config, 225	deletes a security map for the specified connector
delete-connector-connection-pool, 227	connection pool, 233
delete-connector-resource, 230	deletes an existing configuration, 225
delete-connector-security-map, 233	deletes tables in HADB, 25
delete-custom-resource, 236	deletes the cluster or server instance from a load
delete-domain, 239	balancer, 251
delete-file-user, 240	deletes the configuration information created in
delete-http-health-checker, 243	domain.xml for the connector module, 310
delete-http-lb, 246	deletes the given domain, 239
delete-http-lb-config, 248	deletes the instance that is not running., 260
delete-http-lb-ref, 251	deletes the node agent and its associated directory
delete-http-listener, 254	structure, 298
delete-iiop-listener, 257	deletes the profiler element, 307
delete-instance, 260	deletes the SSL element in the selected HTTP listener,
delete-javamail-resource, 262	IIOP listener, or IIOP service, 316
delete-jdbc-connection-pool, 265	deletes the transformation rule of a given web
delete-jdbc-resource, 268	service, 324
delete-jms-host, 274	deploy, 330
delete-jms-resource, 277	deploy-jbi-service-assembly, 342
delete-jmsdest, 271	deploydir, 336
delete-jndi-resource, 280	deploys a service assembly into the JBI
delete-jvm-options command, 283	environment, 342
delete-lifecycle-module, 286	deploys an exploded format of application archive, 336
delete-management-rule, 289	deploys the specified component, 330
delete-mbean, 292	disable, 345
delete-message-security-provider, 295	disable-http-lb-application, 348
delete-node-agent, 298	disable-http-lb-server, 351
delete-node-agent-config, 299	disables a sever or cluster managed by a load
delete-password-alias, 302	balancer, 351
delete-persistence-resource, 304	disables an application managed by a load
delete-profiler, 307	balancer, 348
delete-resource-adapter-config, 310	disables the component, 345
delete-resource-ref, 313	display-error, 354, 357
delete-ssl, 316	display-license, 360
delete-system-property, 319	display-log, 363
delete-transformation-rule, 324	displays a summary of list of severity's and
delete-virtual-server, 327	warnings, 357
deletes a cluster, 222	displays distribution of errors from instance server.log
deletes a custom MBean, 292	at module level, 354

displays monitoring data for commonly-used generates JAX-WS portable artifacts used in JAX-WS Application Server components, 593 web services, 759 displays the asadmin utility commands, 416 generates reports that can help diagnose application displays the license information, 360 server malfunctioning, 387 displays the status of the deployed component, 626 generates stubs, ties, serializers, and WSDL files used in displays the version information, 720 JAX-RPC clients and services, 752, 761 domain, 771 get, 394 Domain Administration Server of the specified get-client-stubs, 411 domain, 680 get-health, 414 domain.xml file, 163, 183, 283 gets all audit modules and displays them, 461 dotted-names, 772 gets all connector resources, 479 dynamically installs any updated components, 748 gets all custom resources, 485 gets all IDBC resources, 526 gets all the administered objects, 455 gets connector connection pools that have been Ε created, 477 enable, 367 gets the access control lists for the named instance, 454 enable-http-lb-application, 370 gets the values of the monitorable or configurable enable-http-lb-server, 373 attributes, 394 enables a previously-disabled application managed by a load balancer, 370 enables a previously disabled sever or cluster managed by a load balancer, 373 Н enables administrators to delete a provider-config help, 416 sub-element for the given message layer HTTP load balancer., 774 (message-security-config element of domain.xml), 295 enables configuration of parameters related to session persistence, 33 П enables the component, 367 install-jbi-component, 430 export, 376 install-jbi-shared-library, 434 export-http-lb-config, 377 install-license, 437 exports the load balancer configuration to a file, 377 installs a service engine or binding component into the IBI environment, 430 installs a shared library into the JBI environment, 434 installs the license file, 437 F instance, 773 flush-jmsdest, 381 G jms-ping, 438 generate-diagnostic-report, 387 jspc, 741 generate-jvm-report, 391

L list-password-aliases, 558 list-resource-adapter-configs, 565 launches the Application Client Container and invokes list-resource-refs, 568 the client application packaged in the application IAR file., 724 list-sub-components, 571 list-system-properties, 573 launches the Jakarta Ant tool, 729 list-timers, 579 lets you log in to a domain, 587 list, 441, 560 list-transformation-rules, 582 list-virtual-servers, 584 list-acls, 454 lists a load balancer, 498 list-admin-objects, 455 lists all backups, 467 list-application-refs, 458 lists all existing configurations, 474 list-audit-modules, 461 lists all existing JNDI resources, 541 list-auth-realms, 464 lists all JDBC connection pools, 524 list-backups, 467 lists all of the timers owned by server instance(s), 579 list-clusters, 468 list-components, 471 lists all password aliases, 558 lists all the instances along with their status, 507 list-configs, 474 lists all the persistence resources, 560 list-connector-connection-pools, 477 lists all the transformation rules of a given webservice. If list-connector-resources, 479 the webservice name option is omitted, then all the list-connector-security-maps, 482 list-custom-resources, 485 transformation rules will be listed, 582 list-domains, 488 lists deployed components, 471 list-file-groups, 489 lists EJBs or Servlets in deployed module or module of deployed application, 571 list-file-users, 492 lists load balancer configurations list-http-lb-configs, 495 list-http-lb-configs, 495 list-http-lbs, 498 list-http-listeners, 501 lists the authentication realms, 464 lists the binding components installed on the specified list-iiop-listeners, 504 list-instances, 507 target, 512 list-javamail-resources, 509 lists the configurable elements, 441 lists the custom mbeans for a given target, 549 list-jbi-binding-components, 512 list-jbi-service-assemblies, 515 lists the domains in the specified domain directory, 488 lists the existing application references, 458 list-jbi-service-engines, 518 list-jbi-shared-libraries, 521 lists the existing clusters, 468 list-jdbc-connection-pools, 524 lists the existing HTTP listeners, 501 list-jdbc-resources, 526 lists the existing IIOP listeners, 504 list-jms-hosts, 532 lists the existing JavaMail session resources, 509 list-jms-resources, 535 lists the existing JMS hosts, 532 list-jmsdest, 529 lists the existing JMS physical destinations, 529 list-jndi-entries, 538 lists the existing references to a resource, 568 list-jndi-resources, 541 lists the existing virtual servers, 584 list-lifecycle-modules, 544 lists the file groups, 489 list-management-rules, 547 lists the JBI shared libraries that are installed into the JBI list-mbeans, 549 Environment, 521 list-node-agents, 555 lists the JMS resources, 535

lists the lifecycle modules, 544
lists the management rules, 547
lists the names of all the resource adapter configs created, 565
lists the node agents along with their status, 555
lists the security maps belonging to the specified connector connection pool, 482
lists the service assemblies installed into the JBI environment, 515
lists the service engines installed on the specified target, 518
loadbalancer, 774
log application server events., 775
logging, 775
login, 587

M

manages and facilitates remote server instances.., 777
manually recovers pending transactions, 605
marks a variable name for automatic export to the
environment of subsequent commands in
multimode, 376
message-security-config element, 163
migrate-timers, 590
migrates the configuration of a previously installed Sun
Java System Application Server, 736
monitor, 593
monitor application server runtime., 776
monitoring, 776
moves a timer when a server instance stops, 590
multimode, 598

N

node-agent - manages and facilitates remote server instances., 777

D

package-appclient, 744

packs the application client container libraries and jar files, 744
passwords, 778
performs a backup on the domain, 20
ping-connection-pool, 599
precompiles JSP source files into servlets, 741
provider-configelement, 163
provides information on the cluster health, 414
provides the complete call flow/path of a request, 650
publishes the web service artifacts to registries., 602
purges messages in a JMS destination, 381

R

reads a WAR file and the jaxrpc-ri.xml file and generates another WAR file that is ready for deployment, 756 recover transactions, 605 registers a JNDI resource, 141 registers a persistence resourcecreate-persistence-resource, create-persistence-resource, 176 registers the connector resource with the specified JNDI name, 67 registers the JDBC connection pool, 121 registers the resource in the XML file specified, 14 remove-ha-cluster, 608 removes a custom resource, 236 removes a deployed component, 691 removes a JavaMail session resource, 262 removes a ICBC resource, 268 removes a JMS host, 274 removes a JMS physical destination, 271 removes a IMS resource, 277 removes a INDI resource, 280 removes a node agent from a domain, 299 removes a persistence resource, 304 removes a reference to a resource, 313 removes a reference to an application, 213 removes a specified management rule, 289 removes a virtual server, 327 removes an HTTP listener, 254 removes an IIOP listener, 257

removes JVM options from the Java configuration or profiler elements of the domain.xml file, 283	shows detailed information about a specified shared library, 638
removes one or more variables from the multimode	shows detailed information about the specified binding
environment, 709	component, 629
removes one system property of the domain,	shows detailed information about the specified service
configuration, cluster, or server instance, at a	engine, 635
time, 319	shows the threads, classes and memory for a given
removes the administered object with the specified	target instance, 391
JNDI name, 210	shut-down-jbi-component, 642
removes the connector resource with the specified JNDI	shut-down-jbi-service-assembly, 645
name, 230	shutdown, 641
removes the lifecycle module, 286	shuts down a JBI service assembly on the specified
removes the named authentication realm, 219	target, 645
removes the named file user, 240	shuts down a service engine or a binding component on
removes the specified connector connection pool, 227	the specified target, 642
removes the specified JDBC connection pool, 265	start-appserv, 648
resources, 779	start-callflow-monitoring -provides the complete call
restore-domain, 611	flow/path of a request., 650
restores files from backup, 611	start-cluster, 653
retrieves the client stub JAR, 411	start-domain, 658
returns an HA cluster to non-HA status, 608	start-instance, 660
returns list of configured web service registry access	start-instance, 660 start-jbi-component, 663
points, 563	start-jbi-service-assembly, 666
	start-node-agent, 669
	start-database, 656
	starts a cluster, 653
S	starts a domain, 658
schemagen, 746	starts a node agent, 669
secure and administer application server., 780	starts a server instance, 660
security, 780	starts a service assembly on the specified target, 666
security credentials., 778	
security service, 163	starts a service engine or a binding component on the specified target, 663
server-side Java applications and Web services., 768	starts the bundled Java DB, 656
set, 615	
sets load balancing weights for clustered instances, 37	starts the domains in the specified domains
sets the monitoring or maxhistorysize attributes of a	directory, 648
deployed webservice, 40	stop-appserv, 672
sets the values of attributes, 615	stop-callflow-monitoring -Disables collection of call
show-component-status, 626	flow information., 673
show-jbi-binding-component, 629	stop-cluster, 676
show-jbi-service-assembly, 632	stop-domain, 680
show-jbi-service-engine, 635	stop-instance, 681
show-jbi-shared-library, 638	stop-jbi-component, 684
shows detailed information about a specified service	stop-jbi-service-assembly, 687
assembly, 632	stop-node-agent, 690

stop-database, 679
stops a cluster, 676
stops a node agent, 690
stops a server instance, 681
stops a service assembly on the specified target, 687
stops a service engine or a binding component on the specified target, 684
stops the bundled Java DB, 679
stops the domains in the specified domains directory, 672
stores the database metadata (schema) in a file for use in mapping and execution, 738
syntax., 772

T

tests that a connection pool is usable, 599 the default administrative domain., 771 transforms, or binds, a source XML schema to a set of JAXB content classes in the Java programming language, 763

U

undeploy, 691 undeploy-jbi-service-assembly, 695 undeploys a service assembly on the specified target, 695 uninstall-jbi-component, 701 uninstall-jbi-shared-library, 704 uninstalls a service engine or binding component on the specified target, 701 uninstalls a shared library on the specified target, 704 unpublishes the web service artifacts from the registries, 707 unset, 709 update-connector-security-map, 710 update-file-user, 713 update-password-alias, 716 updates a current file user as specified, 713 updates a password alias, 716 updatetool, 748

utility for performing administrative tasks for the Sun Java System Application Server, 726

V

validates the J2EE Deployment Descriptors against application server DTDs, 749 verifier, 749 verifies the content of the domain.xml file, 719 verify-domain-xml, 719 version, 720

W

ws, 761 wscompile, 752 wsdeploy, 756 wsgen, 759

X

xjc, 763