<?xml version="1.0" encoding="UTF-8"?>
<!--
 The contents of this file are subject to the terms
 of the Common Development and Distribution License
 (the License). You may not use this file except in
 compliance with the License.
 You can obtain a copy of the license at

 https://glassfish.dev.java.net/public/CDDLv1.0.html or
 glassfish/bootstrap/legal/CDDLv1.0.txt.
 See the License for the specific language governing
 permissions and limitations under the License.

 When distributing Covered Code, include this CDDL

 Header Notice in each file and include the License file
 at glassfish/bootstrap/legal/CDDLv1.0.txt.
 If applicable, add the following below the CDDL Header,
 with the fields enclosed by brackets [] replaced by
 you own identifying information:
 "Portions Copyrighted [year] [name of copyright owner]"

 Copyright 2006 Sun Microsystems, Inc. All rights reserved.-->
<!--
  A domain configuration instance document is validated against this DTD. -->
<!-- ENTITIES -->
<!-- boolean

  Used in:
    access-log, admin-object-resource, appclient-module,
    application-ref, availability-service, cluster, config,
    connector-connection-pool, connector-module, connector-resource,
    custom-resource, das-config, diagnostic-service,
    ejb-container-availability, ejb-module, event, extension-module,
    external-jndi-resource, http-access-log, http-file-cache,
    http-listener, http-protocol, iiop-listener, iiop-service,
    j2ee-application, java-config, jdbc-connection-pool,
    jdbc-resource, jms-availability, jms-service, jmx-connector,
    lb-config, lifecycle-module, load-balancer, log-service,
    mail-resource, management-rule, management-rules, mbean,
    node-agent, persistence-manager-factory-resource, profiler,

```
    resource-ref, security-service, server-ref, ssl,
    transaction-service, transformation-rule,
    web-container-availability, web-module, web-service-endpoint
-->
<!ENTITY % boolean "(yes | no | on | off | 1 | 0 | true | false)">

<!-- isolation

  Used in:
    jdbc-connection-pool
-->
<!ENTITY % isolation
    "(read-uncommitted | read-committed | repeatable-read | serializable)">


<!-- validation-level

  Used in:
    das-config
-->
<!ENTITY % validation-level "(full | parsing | none)">

<!-- object-type
    defines the type of the resource. It can be:
    system-all
        These are system resources for all instances and DAS
    system-admin
        These are system resources only in DAS
    system-instance
        These are system resources only in instances (and not DAS)
    user
        User resources (This is the default for all elements)

  Used in:
    admin-object-resource, connector-module, connector-resource,
    custom-resource, ejb-module, extension-module,
    external-jndi-resource, j2ee-application, jdbc-resource,
    lifecycle-module, mail-resource, mbean,
    persistence-manager-factory-resource, resource-adapter-config,
    web-module
-->
```

```
<!ENTITY % object-type "(system-all | system-admin | system-instance | user)">

<!-- rjmx-protocol
    SE/EE related ENTITIES: This will define the available JSR 160
    connector transport protocols.

  Used in:
    jmx-connector
-->
<!ENTITY % rjmx-protocol "(rmi_jrmp | rmi_iiop | jmxmp)">

<!-- monitoring-level
    monitoring-level controls the amount of monitoring data collected
    and exposed to clients
    OFF
        no monitoring/statistical data is exposed to the clients.
    LOW
        SE/EE only
    HIGH
        maximum data is gathered and released.

  Used in:
    module-monitoring-levels, web-service-endpoint
-->
<!ENTITY % monitoring-level "(OFF | LOW | HIGH)">

<!-- session-save-frequency

  Used in:
    web-container-availability
-->
<!ENTITY % session-save-frequency "(web-method | time-based | on-demand)">

<!-- session-save-scope

  Used in:
    web-container-availability
-->
<!ENTITY % session-save-scope
    "(session | modified-session | modified-attribute)">
```

```
<!-- apply-to-type

  Used in:
    transformation-rule
-->
<!ENTITY % apply-to-type "(request | response | both)">

<!-- lb-policy-type

  Used in:
    cluster-ref
-->
<!ENTITY % lb-policy-type
    "(round-robin | weighted-round-robin | user-defined)">


<!-- event-type

  Used in:
    event
-->
<!ENTITY % event-type
    "(log | timer | trace | monitor | cluster | lifecycle | notification)">


<!-- message-layer

  Used in:
    message-security-config
-->
<!ENTITY % message-layer "(SOAP | HttpServlet)">

<!-- log-level
    Configure the Log Levels for Various Loggers in the SUN ONE
    Modules. The Default level is set to INFO, The log levels can be
    changed using one of the seven levels. Please refer JSR 047 to
    understand the Log Levels.

    The Logs can be completely turned off by using 'OFF' value. The names of
    the module loggers are self-explanatory
```

```
  Used in:
    diagnostic-service, event, module-log-levels
-->
<!ENTITY % log-level
    "(FINEST | FINER | FINE | CONFIG | INFO | WARNING | SEVERE | OFF)">



<!-- ELEMENTS -->

<!-- domain
    Top level Domain Element that includes applications, resources,
    configs, servers, clusters and node-agents, load balancer
    configurations and load balancers. node-agents and load balancers
    are SE/EE related entities only.

  attributes
    application-root
        for PE this defines the location where applications are
        deployed
    locale
        If present, overrides OS locale setting.
    log-root
        specifies where the server instance's log files are kept,
        including HTTP access logs, server logs, and transaction
        logs. Default is $INSTANCE-ROOT/logs
-->
<!ELEMENT domain
    (applications?, resources?, configs, servers, clusters?, node-agents?,
    lb-configs?, load-balancers?, system-property*, property*)>


<!ATTLIST domain
    application-root CDATA #IMPLIED
    log-root CDATA #IMPLIED
    locale CDATA #IMPLIED>


<!-- configs
```

```
  Used in:
    domain
-->
<!ELEMENT configs (config+)>


<!-- servers

  Used in:
    domain
-->
<!ELEMENT servers (server*)>


<!-- clusters

  Used in:
    domain
-->
<!ELEMENT clusters (cluster*)>


<!-- node-agents

  Used in:
    domain
-->
<!ELEMENT node-agents (node-agent*)>


<!-- lb-configs

  Used in:
    domain
-->
<!ELEMENT lb-configs (lb-config*)>


<!-- applications
    Various types of applications that can be deployed on Sun ONE
```

```
    Application Server instance

  Used in:
    domain
-->
<!ELEMENT applications
    ((lifecycle-module | j2ee-application | ejb-module | web-module |
    connector-module | appclient-module | mbean | extension-module)*)>



<!-- lifecycle-module

  attributes
    class-name
        fully qualified name of the startup class.
    classpath
        where this module is actually located, if it is not under
        applications-root
    enabled
        boolean attribute. If set to "false" this module will not be
        loaded at server start up.
    is-failure-fatal
        if true, aborts server start up if this module does not load
        properly.
    load-order
        integer value that can be used to force the order in which
        deployed lifecycle modules are loaded at server start up.
        Smaller numbered modules get loaded sooner. Order is
        unspecified if two or more lifecycle modules have the same
        load-order value.
    name
        unqiue identifier for the deployed server lifecycle event
        listener module.

  Used in:
    applications
-->
<!ELEMENT lifecycle-module (description?, property*)>

<!ATTLIST lifecycle-module
```

```
  name CDATA #REQUIRED
  class-name CDATA #REQUIRED
  classpath CDATA #IMPLIED
  load-order CDATA #IMPLIED
  is-failure-fatal %boolean; "false"
  object-type %object-type; "user"
  enabled %boolean; "true">


<!-- j2ee-application

  attributes
    availability-enabled
      This boolean flag controls whether availability is enabled
      for SFSB checkpointing (and potentially passivation). If this
      is "false", then all SFSB checkpointing is disabled for
      either the given j2ee app or the given ejb module. If it is
      "true" (and providing that all the availability-enabled
      attributes above in precedence are also "true", then the j2ee
      app or stand-alone ejb modules may be ha enabled.
      Finer-grained control exists at lower level inside each bean.
      If this attribute is missing, it defaults to "false".
    directory-deployed
      This attribute indicates whether the application has been
      deployed to a directory or not
    java-web-start-enabled
      This attribute indicates whether Java Web Start access is
      permitted to eligible application client(s) in this module
    libraries
      System dependent path separator [: for Unix/Solaris/Linux and
      ; for Windows] separated list of jar paths. These paths could
      be either relative [relative to
      {com.sun.aas.instanceRoot}/lib/applibs] or absolute paths.
      These dependencies appears *after* the libraries defined in
      classpath-prefix in the java-config and *before* the
      application server provided over-rideable jar set. The
      libraries would be made available to the application in the
      order in which they were specified.

  Used in:
    applications
```

```
-->
<!ELEMENT j2ee-application (description?, web-service-endpoint*, property*)>

<!ATTLIST j2ee-application
   name CDATA #REQUIRED
   location CDATA #REQUIRED
   object-type %object-type; "user"
   enabled %boolean; "true"
   libraries CDATA #IMPLIED
   availability-enabled %boolean; "false"
   directory-deployed %boolean; "false"
   java-web-start-enabled %boolean; "true">


<!-- ejb-module

  attributes
    availability-enabled
       This boolean flag controls whether availability is enabled
       for SFSB checkpointing (and potentially passivation). If this
       is "false", then all SFSB checkpointing is disabled for
       either the given j2ee app or the given ejb module. If it is
       "true" (and providing that all the availability-enabled
       attributes above in precedence are also "true", then the j2ee
       app or stand-alone ejb modules may be ha enabled.
       Finer-grained control exists at lower level inside each bean.
       If this attribute is missing, it defaults to "false".
    directory-deployed
       This attribute indicates whether the application has been
       deployed to a directory or not
    libraries
       System dependent path separator [: for Unix/Solaris/Linux and
       ; for Windows] separated list of jar paths. These paths could
       be either relative [relative to
       {com.sun.aas.instanceRoot}/lib/applibs] or absolute paths.
       These dependencies appears *after* the libraries defined in
       classpath-prefix in the java-config and *before* the
       application server provided over-rideable jar set. The
       libraries would be made available to the application in the
       order in which they were specified.
```

```
  Used in:
    applications
-->
<!ELEMENT ejb-module (description?, web-service-endpoint*, property*)>

<!ATTLIST ejb-module
    name CDATA #REQUIRED
    location CDATA #REQUIRED
    object-type %object-type; "user"
    enabled %boolean; "true"
    libraries CDATA #IMPLIED
    availability-enabled %boolean; "false"
    directory-deployed %boolean; "false">


<!-- web-module

  attributes
    availability-enabled
        This boolean flag controls whether availability is enabled
        for HTTP Session Persistence. If this is "false", then all
        session persistence is disabled for the given web module. If
        it is "true" (and providing that all the availability-enabled
        attributes above in precedence are also "true", then the web
        module may be ha enabled. Finer-grained control exists at
        lower level (see sun-web.xml). If this attribute is missing,
        it defaults to "false".
    context-root
        context-root must match the pattern for the hpath production
        in RFC 1738 which can be found at:
        http://www.w3.org/Addressing/rfc1738.txt. This is flattened
        to the following regular expression in XML Schema's pattern
        language:
        ([a-zA-Z0-9$\-_.+!*'(),]|%[0-9A-Fa-f][0-9A-Fa-f]|;|:|&|=)*(/([
        -zA-Z0-9$\-_.+!*'(),]|%[0-9A-Fa-f][0-9A-Fa-f]|;|:|&|=)*)*
        Note that this includes the null or empty context root and
        permits but does not require a context root to start with the
        '/' character (including a context root which is simply the
        '/' character).
    directory-deployed
        This attribute indicates whether the application has been
```

```
      deployed to a directory or not
    libraries
      System dependent path separator [: for Unix/Solaris/Linux and
      ; for Windows] separated list of jar paths. These paths could
      be either relative [relative to
      {com.sun.aas.instanceRoot}/lib/applibs] or absolute paths.
      These dependencies appears *after* the libraries defined in
      classpath-prefix in the java-config and *before* the
      application server provided over-rideable jar set. The
      libraries would be made available to the application in the
      order in which they were specified.

  Used in:
    applications
-->
<!ELEMENT web-module (description?, web-service-endpoint*, property*)>

<!ATTLIST web-module
    name CDATA #REQUIRED
    context-root CDATA #REQUIRED
    location CDATA #REQUIRED
    object-type %object-type; "user"
    enabled %boolean; "true"
    libraries CDATA #IMPLIED
    availability-enabled %boolean; "false"
    directory-deployed %boolean; "false">


<!-- connector-module

  Used in:
    applications
-->
<!ELEMENT connector-module (description?, property*)>

<!ATTLIST connector-module
    name CDATA #REQUIRED
    location CDATA #REQUIRED
    object-type %object-type; "user"
    enabled %boolean; "true"
    directory-deployed %boolean; "false">
```

```
<!-- appclient-module

  attributes
    java-web-start-enabled
        This attribute indicates whether Java Web Start access is
        permitted to eligible application client(s) in this module

  Used in:
    applications
-->
<!ELEMENT appclient-module (description?, property*)>

<!ATTLIST appclient-module
    name CDATA #REQUIRED
    location CDATA #REQUIRED
    directory-deployed %boolean; "false"
    java-web-start-enabled %boolean; "true">


<!-- resources
    J2EE Applications look up resources registered with the
    Application server, using portable JNDI names.

  Used in:
    domain
-->
<!ELEMENT resources
    ((custom-resource | external-jndi-resource | jdbc-resource | mail-resource
    | persistence-manager-factory-resource | admin-object-resource |
    connector-resource | resource-adapter-config | jdbc-connection-pool |
    connector-connection-pool)*)>



<!-- description
    Textual description of a configured entity

  Used in:
    admin-object-resource, appclient-module,
```

```
    connector-connection-pool, connector-module, connector-resource,
    custom-resource, ejb-module, event, extension-module,
    external-jndi-resource, j2ee-application, jdbc-connection-pool,
    jdbc-resource, lifecycle-module, mail-resource, management-rule,
    mbean, persistence-manager-factory-resource, property,
    system-property, web-module
-->
<!ELEMENT description (#PCDATA)>


<!-- custom-resource
    custom (or generic) resource managed by a user-written factory
    class.

  attributes
    jndi-name
        JNDI name for generic resource, the fully qualified type of
        the resource and whether it is enabled at runtime

  Used in:
    resources
-->
<!ELEMENT custom-resource (description?, property*)>

<!ATTLIST custom-resource
    jndi-name CDATA #REQUIRED
    res-type CDATA #REQUIRED
    factory-class CDATA #REQUIRED
    object-type %object-type; "user"
    enabled %boolean; "true">


<!-- external-jndi-resource
    resource residing in an external JNDI repository

  Used in:
    resources
-->
<!ELEMENT external-jndi-resource (description?, property*)>

<!ATTLIST external-jndi-resource
```

```
    jndi-name CDATA #REQUIRED
    jndi-lookup-name CDATA #REQUIRED
    res-type CDATA #REQUIRED
    factory-class CDATA #REQUIRED
    object-type %object-type; "user"
    enabled %boolean; "true">


<!-- jdbc-resource
    JDBC javax.sql.(XA)DataSource resource definition

  Used in:
    resources
-->
<!ELEMENT jdbc-resource (description?, property*)>

<!ATTLIST jdbc-resource
    jndi-name CDATA #REQUIRED
    pool-name CDATA #REQUIRED
    object-type %object-type; "user"
    enabled %boolean; "true">


<!-- mail-resource
    The mail-resource element describes a javax.mail.Session resource

  attributes
    host
        ip V6 or V4 address or hostname.

  Used in:
    resources
-->
<!ELEMENT mail-resource (description?, property*)>

<!ATTLIST mail-resource
    jndi-name CDATA #REQUIRED
    store-protocol CDATA "imap"
    store-protocol-class CDATA "com.sun.mail.imap.IMAPStore"
    transport-protocol CDATA "smtp"
    transport-protocol-class CDATA "com.sun.mail.smtp.SMTPTransport"
```

```
    host CDATA #REQUIRED
    user CDATA #REQUIRED
    from CDATA #REQUIRED
    debug %boolean; "false"
    object-type %object-type; "user"
    enabled %boolean; "true">


<!-- persistence-manager-factory-resource
    Persistence Manager runtime configuration.

  attributes
    factory-class
        Class that creates persistence manager instance.
    jdbc-resource-jndi-name
        jdbc resource with which database connections are obtained.
    jndi-name
        JNDI name for this resource

  Used in:
    resources
-->
<!ELEMENT persistence-manager-factory-resource (description?, property*)>

<!ATTLIST persistence-manager-factory-resource
    jndi-name CDATA #REQUIRED
    factory-class CDATA
"com.sun.jdo.spi.persistence.support.sqlstore.impl.PersistenceManagerFactoryImpl"
    jdbc-resource-jndi-name CDATA #IMPLIED
    object-type %object-type; "user"
    enabled %boolean; "true">


<!-- admin-object-resource
    The admin-object-resource element describes a administered object
    for a inbound resource adapter.

  attributes
    jndi-name
        JNDI name for this resource
    res-adapter
```

```
        Name of the inbound resource adapter.
    res-type
        Interface definition for the administered object

  Used in:
    resources
-->
<!ELEMENT admin-object-resource (description?, property*)>

<!ATTLIST admin-object-resource
    jndi-name CDATA #REQUIRED
    res-type CDATA #REQUIRED
    res-adapter CDATA #REQUIRED
    object-type %object-type; "user"
    enabled %boolean; "true">


<!-- connector-resource

  Used in:
    resources
-->
<!ELEMENT connector-resource (description?, property*)>

<!ATTLIST connector-resource
    jndi-name CDATA #REQUIRED
    pool-name CDATA #REQUIRED
    object-type %object-type; "user"
    enabled %boolean; "true">


<!-- resource-adapter-config
    This element is for configuring the resource adapter. These
    values (properties) over-rides the default values present in
    ra.xml. The name attribute has to be unique . It is optional for
    PE. It is used mainly for EE.

  Used in:
    resources
-->
<!ELEMENT resource-adapter-config (property*)>
```

```
<!ATTLIST resource-adapter-config
    name CDATA #IMPLIED
    thread-pool-ids CDATA #IMPLIED
    object-type %object-type; "user"
    resource-adapter-name CDATA #REQUIRED>


<!-- config
    The configuration defines the configuration of a server instance
    that can be shared by other server instances. The
    availability-service and are SE/EE only.

  attributes
    dynamic-reconfiguration-enabled
        When set to "true" then any changes to the system (e.g.
        applications deployed, resources created) will be
        automatically applied to the affected servers without a
        restart being required. When set to "false" such changes will
        only be picked up by the affected servers when each server
        restarts.

  Used in:
    configs
-->
<!ELEMENT config
    (http-service, iiop-service, admin-service, connector-service?,
    web-container, ejb-container, mdb-container, jms-service?, log-service,
    security-service, transaction-service, monitoring-service,
    diagnostic-service?, java-config, availability-service?, thread-pools,
    alert-service?, group-management-service?, management-rules?,
    system-property*, property*)>


<!ATTLIST config
    name CDATA #REQUIRED
    dynamic-reconfiguration-enabled %boolean; "true">


<!-- alert-service
    The Alert service provides a mechanism for users to register for
```

```
    and receive alerts. The alert service collects together a set of
    alert subscriptions

  Used in:
    config
-->
<!ELEMENT alert-service (alert-subscription*, property*)>


<!-- alert-subscription
    alert subscription details a specific subscription. The
    subscription comprises the configuration of a specific listener,
    and a filter to be applied.

  attributes
    name
        The unique name identifying a particular alert service.

  Used in:
    alert-service
-->
<!ELEMENT alert-subscription (listener-config, filter-config?)>

<!ATTLIST alert-subscription
    name CDATA #REQUIRED>


<!-- listener-config
    connects a specific listener class with specific managed objects

  attributes
    listener-class-name
        The name of a class that can act as a listener for alerts.
        Non-empty string containing a Java class name.
    subscribe-listener-with
        A list of managed object names that the listener should be
        subscribed to. A non-empty, comma separated list.

  Used in:
    alert-subscription
-->
```

```
<!ELEMENT listener-config (property*)>

<!ATTLIST listener-config
   listener-class-name CDATA #REQUIRED
   subscribe-listener-with CDATA #REQUIRED>


<!-- filter-config
   filter-config provides the means of specifying a filter to be
   applied to alerts

  attributes
   filter-class-name
      The name of a class that can act as a filter. Non-empty
      string containing a Java class name.

  Used in:
   alert-subscription
-->
<!ELEMENT filter-config (property*)>

<!ATTLIST filter-config
   filter-class-name CDATA #REQUIRED>


<!-- http-service

  Used in:
   config
-->
<!ELEMENT http-service
   (access-log?, http-listener+, virtual-server+, request-processing?,
   keep-alive?, connection-pool?, http-protocol?, http-file-cache?,
   property*)>



<!-- access-log

  attributes
   format
```

```
      The global format for the access log rotation-policy The
      policy based on which the log rotation would be done . At
      this time only time based rotation is enabled.
    rotation-enabled
      The flag for enabling the access-log rotation
    rotation-interval-in-minutes
      The time interval in minutes between two successive rotations
      of the access logs.
    rotation-suffix
      The suffix to be added to the access-log name after rotation.
      Acceptable values include those supported by
      java.text.SimpleDateFormat and
      "%YYYY;%MM;%DD;-%hh;h%mm;m%ss;s".

  Used in:
    http-service
-->
<!ELEMENT access-log EMPTY>

<!ATTLIST access-log
    format CDATA "%client.name% %auth-user-name% %datetime% %request%
%status% %response.length%"
    rotation-policy (time) "time"
    rotation-interval-in-minutes CDATA "1440"
    rotation-suffix CDATA "yyyyMMdd-HH'h'mm'm'ss's'"
    rotation-enabled %boolean; "true">


<!-- http-listener

  attributes
    acceptor-threads
      Number of acceptor threads for the listen socket. The
      recommended value is the number of processors in the machine.
    address
      IP address of the listen socket. Can be in dotted-pair or
      IPv6 notation. Can also be any for INADDR-ANY. Configuring a
      listen socket to listen on any is required if more than one
      http-listener is configured to it.
    blocking-enabled
      Enables blocking for the listen and external ports.
```

default-virtual-server
The id attribute of the default virtual server for this particular connection group.
external-port
The port at which the user makes a request , typically a proxy server port.
family
Specified the family of addresses either inet or ncsa
id
Unique identifier for http listener.
port
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.
redirect-port
if the connector is supporting non-SSL requests and a request is received for which a matching security-constraint requires SSL transport catalina will automatically redirect the request to the port number specified here
security-enabled
Determines whether the http listener runs SSL. You can turn SSL2 or SSL3 on or off and set ciphers using an ssl element. The enable-ssl in the protocol element should be set to true for this setting to work.
server-name
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 doesnt 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 you append a colon and port number, that port will be used in URLs the server sends to the client.
xpowered-by
The Servlet 2.4 spec defines a special X-Powered-By: Servlet/2.4 header, which containers may add to servlet-generated responses. This is complemented by the JSP 2.0 spec, which defines a X-Powered-By: JSP/2.0 header to be added (on an optional basis) to responses utilizing JSP technology. The goal of these headers is to aid in gathering statistical data about the use of Servlet and JSP technology.

```
        If true, these headers will be added.

  Used in:
    http-service
-->
<!ELEMENT http-listener (ssl?, property*)>

<!ATTLIST http-listener
    id CDATA #REQUIRED
    address CDATA #REQUIRED
    port CDATA #REQUIRED
    external-port CDATA #IMPLIED
    family (inet | ncsa) "inet"
    blocking-enabled %boolean; "false"
    acceptor-threads CDATA "1"
    security-enabled %boolean; "false"
    default-virtual-server CDATA #REQUIRED
    server-name CDATA #REQUIRED
    redirect-port CDATA #IMPLIED
    xpowered-by %boolean; "true"
    enabled %boolean; "true">



<!-- ssl
    Define SSL processing parameters

  attributes
    cert-nickname
        nickname of the server certificate in the certificate
        database or the PKCS#11 token. In the certificate, the name
        format is tokenname:nickname. Including the tokenname: part
        of the name in this attribute is optional.
    client-auth-enabled
        Determines whether SSL3 client authentication is performed on
        every request, independent of ACL-based access control.
    ssl2-ciphers
        A comma-separated list of the SSL2 ciphers used, with the
        prefix + to enable or - to disable, for example +rc4. Allowed
        values are rc4, rc4export, rc2, rc2export, idea, des,
        desede3. If no value is specified, all supported ciphers are
        assumed to be enabled. NOT Used in PE
```

```
    ssl2-enabled
        Determines whether SSL2 is enabled. NOT Used in PE. SSL2 is
        not supported by either iiop or web-services. When this
        element is used as a child of the iiop-listener element then
        the only allowed value for this attribute is "false".
    ssl3-enabled
        Determines whether SSL3 is enabled.

        If both SSL2 and SSL3 are enabled for a virtual server, the server
        tries SSL3 encryption first. If that fails, the server tries SSL2
        encryption.

    ssl3-tls-ciphers
        A comma-separated list of the SSL3 ciphers used, with the
        prefix + to enable or - to disable, for example
        +SSL_RSA_WITH_RC4_128_MD5. Allowed SSL3/TLS values are those
        that are supported by the JVM for the given security provider
        and security service configuration. If no value is specified,
        all supported ciphers are assumed to be enabled.
    tls-enabled
        Determines whether TLS is enabled.
    tls-rollback-enabled
        Determines whether TLS rollback is enabled. TLS rollback
        should be enabled for Microsoft Internet Explorer 5.0 and
        5.5. NOT Used in PE

  Used in:
    http-listener, iiop-listener, jmx-connector, ssl-client-config
-->
<!ELEMENT ssl EMPTY>

<!ATTLIST ssl
    cert-nickname CDATA #REQUIRED
    ssl2-enabled %boolean; "false"
    ssl2-ciphers CDATA #IMPLIED
    ssl3-enabled %boolean; "true"
    ssl3-tls-ciphers CDATA #IMPLIED
    tls-enabled %boolean; "true"
    tls-rollback-enabled %boolean; "true"
    client-auth-enabled %boolean; "false">
```

<!-- virtual-server
Configuration of Virtual Server

Virtualization in Application Server allows multiple URL domains to be served by the same HTTP server process, which is listening on multiple host addresses If an application is available at two virtual servers, they still share same physical resource pools, such as JDBC connection pools.

Sun ONE Application Server allows a list of virtual servers, to be specified along with web-module and j2ee-application elements. This establishes an association between URL domains, represented by the virtual server and the web modules (standalone web modules or web modules inside the ear file)

attributes
default-web-module
stand alone web module associated with this virtual server by default.
docroot
The location on the filesystem where the files related to the content to be served by this virtual server is stored.
hosts
A comma-separated list of values allowed in the Host request header to select the current virtual server. Each Virtual Server that is configured to the same Connection Group must have a unique hosts value for that group.
http-listeners
A comma-separated list of http-listener id(s), Required only for a Virtual Server that is not the default virtual server.
id
Virtual server ID. This is a unique ID that allows lookup of a specific virtual server. A virtual server ID cannot begin with a number.
log-file
Specifies a log file for virtual-server-specific log messages. Default value is ${com.sun.aas.instanceRoot}/logs/server.log
state
Determines whether a Virtual Server is active (on) or

```
        inactive (off, disable). The default is on (active). When
        inactive, a Virtual Server does not service requests.
        off
            returns a 404: Status code (404) indicating that the
            requested resource is not available
        disabled
            returns a 403: Status code (403) indicating the server
            understood the request but refused to fulfill it.

  Used in:
    http-service
-->
<!ELEMENT virtual-server (http-access-log?, property*)>

<!ATTLIST virtual-server
    id CDATA #REQUIRED
    http-listeners CDATA #IMPLIED
    default-web-module CDATA #IMPLIED
    hosts CDATA #REQUIRED
    state (on | off | disabled) "on"
    docroot CDATA #IMPLIED
    log-file CDATA "${com.sun.aas.instanceRoot}/logs/server.log">


<!-- http-access-log

  attributes
    iponly
        if the IP address of the user agent should be specified or a
        DNL lookup should be done
    log-directory
        location of the access logs specified as a directory.This
        defaults to the domain.log-root, which by default is
        ${INSTANCE_ROOT}/logs. Hence the default value for this
        attribute is ${INSTANCE_ROOT}/logs/access

  Used in:
    virtual-server
-->
<!ELEMENT http-access-log EMPTY>
```

```
<!ATTLIST http-access-log
    log-directory CDATA "${com.sun.aas.instanceRoot}/logs/access"
    iponly %boolean; "true">


<!-- request-processing
    This element provides attributes to configure the request
    processing subsystem in the HTTP service.

  attributes
    header-buffer-length-in-bytes
        The size of the buffer used by the request processing threads
        for reading the request data
    initial-thread-count
        The no of request processing threads when the http service is
        initialized
    request-timeout-in-seconds
        Time after which the request times out
    thread-count
        Max no of request processing threads.
    thread-increment
        The increment in the no of request processing threads when
        the no. of requests reaches the number specified by
        request-threads-init

  Used in:
    http-service
-->
<!ELEMENT request-processing EMPTY>

<!ATTLIST request-processing
    thread-count CDATA "128"
    initial-thread-count CDATA "48"
    thread-increment CDATA "10"
    request-timeout-in-seconds CDATA "30"
    header-buffer-length-in-bytes CDATA "4096">


<!-- keep-alive
    Keep-alive subsystem configuration
```

```
  attributes
    max-connections
       Max no of connection in the Keep Alive mode
    thread-count
       no of Keep Alive threads in the system
    timeout-in-seconds
       Keep Alive timeout , max time a connection can be deemed as
       idle and kept in the keep-alive state

  Used in:
    http-service
-->
<!ELEMENT keep-alive EMPTY>

<!ATTLIST keep-alive
    thread-count CDATA "1"
    max-connections CDATA "256"
    timeout-in-seconds CDATA "30">


<!-- connection-pool

  attributes
    max-pending-count
       Max no of pending connections on the listen socket
    queue-size-in-bytes
       Size in bytes of the Connection queue
    receive-buffer-size-in-bytes
       The buffer size of the receive buffer used by sockets.
    send-buffer-size-in-bytes
       The buffer size of the send buffer used by sockets.

  Used in:
    http-service
-->
<!ELEMENT connection-pool EMPTY>

<!ATTLIST connection-pool
    queue-size-in-bytes CDATA "4096"
    max-pending-count CDATA "4096"
    receive-buffer-size-in-bytes CDATA "4096"
```

```
    send-buffer-size-in-bytes CDATA "8192">


<!-- http-protocol
    HTTP Protocol related settings

  attributes
    default-response-type
        Setting the default response-type. Specified as a semi-colon
        delimited string consisting of content-type, encoding,
        language, charset
    dns-lookup-enabled
        If the DNS name for a particular ip address from which the
        request originates needs to be looked up.
    forced-response-type
        The response type to be forced if the content served cannot
        be matched by any of the MIME mappings for extensions.
        Specified as a semi-colon delimited string consisting of
        content-type, encoding, language, charset
    ssl-enabled
        Globally enables SSL across the server
    version
        The version of the HTTP protocol used by the HTTP Service

  Used in:
    http-service
-->
<!ELEMENT http-protocol EMPTY>

<!ATTLIST http-protocol
    version CDATA "HTTP/1.1"
    dns-lookup-enabled %boolean; "false"
    forced-response-type CDATA "text/html; charset=iso-8859-1"
    default-response-type CDATA "text/html; charset=iso-8859-1"
    ssl-enabled %boolean; "true">


<!-- http-file-cache

  attributes
    file-caching-enabled
```

```
      Enables the caching of file content if the file size is less
      than the one specified ny med-file-size-limit
    file-transmission-enabled
      This is valid on Windows only. Enables the TransmitFileSystem
      call.
    globally-enabled
      globally enables the file cache
    hash-init-size
      Initial no. of hash buckets.
    max-age-in-seconds
      Maximum age of a valid cache entry
    max-files-count
      Maximum no. of files in the file cache.
    medium-file-size-limit-in-bytes
      Maximum size of a cached file that can be stored as a memory
      mapped file.
    medium-file-space-in-bytes
      Total size of all files that are cached as memory mapped
      files.
    small-file-size-limit-in-bytes
      Maximum size of a file that can be read into memory.
    small-file-space-in-bytes
      Total size of the files that are read into memory.

  Used in:
    http-service
-->
<!ELEMENT http-file-cache EMPTY>

<!ATTLIST http-file-cache
    globally-enabled %boolean; "true"
    file-caching-enabled %boolean; "on"
    max-age-in-seconds CDATA "30"
    medium-file-size-limit-in-bytes CDATA "537600"
    medium-file-space-in-bytes CDATA "10485760"
    small-file-size-limit-in-bytes CDATA "2048"
    small-file-space-in-bytes CDATA "1048576"
    file-transmission-enabled %boolean; "false"
    max-files-count CDATA "1024"
    hash-init-size CDATA "0">
```

```
<!-- iiop-service

  Used in:
    config
-->
<!ELEMENT iiop-service (orb, ssl-client-config?, iiop-listener*)>

<!ATTLIST iiop-service
    client-authentication-required %boolean; "false">


<!-- orb
    Orb Configuration properties

  attributes
    max-connections
        maximum number of incoming connections, on all listeners
    message-fragment-size
        GIOPv1.2 messages larger than this will get fragmented.
        Minimum value is 128.
    use-thread-pool-ids
        This would refer to the thread-pool-id(s) defined in the
        thread-pool sub-element of thread-pool-config element in
        server.xml. These would be the threadpool(s) used by the ORB.
        More than one thread-pool-id(s) could be specified by using
        commas to separate the names e.g. orb-thread-pool-1,
        orb-thread-pool-2

  Used in:
    iiop-service
-->
<!ELEMENT orb (property*)>

<!ATTLIST orb
    use-thread-pool-ids CDATA #REQUIRED
    message-fragment-size CDATA "1024"
    max-connections CDATA "1024">


<!-- ssl-client-config
```

```
    ssl-client-config element specifies the SSL configuration when
    the Application Server is making outbound IIOP/SSL connections.

  Used in:
    iiop-service
-->
<!ELEMENT ssl-client-config (ssl)>


<!-- iiop-listener

  children
    ssl
        element specifies optional SSL configuration. Note that the
        ssl2 ciphers are not supported for iiop, and therefore must
        be disabled.

  attributes
    address
        ip V6 or V4 address or hostname.
    enabled
        if false, a configured listener, is disabled
    id
        unique identifier for this listener.
    port
        port number
    security-enabled
        Determines whether the iiop listener runs SSL. You can turn
        SSL2 or SSL3 on or off and set ciphers using an ssl element

  Used in:
    iiop-service
-->
<!ELEMENT iiop-listener (ssl?, property*)>

<!ATTLIST iiop-listener
    id CDATA #REQUIRED
    address CDATA #REQUIRED
    port CDATA "1072"
    security-enabled %boolean; "false"
    enabled %boolean; "true">
```

```
<!-- admin-service
    Admin Service exists in every instance. It is the configuration
    for either a normal server, DAS or PE instance.

  attributes
    type
        an instance can either be of type
        das
            Domain Administration Server in SE/EE or the PE instance
        das-and-server
            same as das
        server
            Any non-DAS instance in SE/EE. Not valid for PE.

  Used in:
    config
-->
<!ELEMENT admin-service (jmx-connector*, das-config?, property*)>

<!ATTLIST admin-service
    type (das | das-and-server | server) "server"
    system-jmx-connector-name CDATA #IMPLIED>


<!-- connector-service
    Configuration of the Connector Container. The attributes
    specified in the connector container would apply to all resource
    adapters deployed in this cluster/server-instance

  attributes
    shutdown-timeout-in-seconds
        integer value (default 30 seconds). Represents the time-out,
        in seconds, that would be allowed by the application server,
        during shutdown, to call the ResourceAdapter.stop() method of
        this connector module's instance to complete.

        Resource Adapters that take longer than the specified
        shutdown-timeout-in-seconds time interval would be ignored and the
        application server shutdown procedure would continue.
```

```
  Used in:
    config
-->
<!ELEMENT connector-service EMPTY>

<!ATTLIST connector-service
    shutdown-timeout-in-seconds CDATA "30">


<!-- jmx-connector
    The jmx-connector element defines the configuration of a JSR 160
    compliant remote JMX Connector.

  attributes
    accept-all
        Determines whether the connection can be made on all the
        network interfaces. A value of false implies that the
        connections only for this specific address will be selected.
        This attribute is ignored for SJS AS 8.1.
    address
        Specifies the IP address or host-name. Ignored for SJS AS 8.1.
    auth-realm-name
        The name of the auth-realm in this config element that
        represents the special administrative realm. All
        authentication (from administraive GUI and CLI) will be
        handled by this realm.
    enabled
        Defines if this connector is enabled. For EE this must be
        enabled.
    name
        name of jmx connector used for identification
    port
        Specifies the port of the jmx-connector-server. Note that
        jmx-service-uRL is a function of protocol, port and address
        as defined by the JSR 160 1.0 Specification.
    protocol
        Defines the protocol that this jmx-connector should support.
        Supported protocols are defined by Entity rjmx-protocol. SJS
        AS 8.1 PE/SE/EE supports "rmi_jrmp" protocol only. Other
```

protocols can be used by user applications independently. For other protocols supported refer to documentation.

security-enabled

Decides whether the transport layer security be used in jmx-connector. If true, configure the ssl element.

Used in:

admin-service, node-agent

-->

<!ELEMENT jmx-connector (ssl?, property*)>

<!ATTLIST jmx-connector
name CDATA #REQUIRED
enabled %boolean; "true"
protocol %rjmx-protocol; "rmi_jrmp"
address CDATA #REQUIRED
port CDATA #REQUIRED
accept-all %boolean; "false"
auth-realm-name CDATA #REQUIRED
security-enabled %boolean; "true">

<!-- das-config

attributes

admin-session-timeout-in-minutes

timeout in minutes indicating the administration gui session timeout.

autodeploy-dir

The source directory (relative to instance root) from which autodeploy service will pick deployable components. You can also specify an absolute directory.

autodeploy-enabled

This will enable the autodeployment service. If true, the service will automatically starts with the admin-server. Auto Deployment is a feature that enables developers to quickly deploy applications and modules to a running application server withoutrequiring the developer to perform an explicit application server restart or separate deployment operation.

autodeploy-jsp-precompilation-enabled

If true, JSPs will be pre compiled during deployment of the

```
      war module(s).
    autodeploy-polling-interval-in-seconds
      The polling interval (in seconds), at the end of which
      autodeployment service will scan the source directory
      (specified by "autodeploy-dir" tag) for any new deployable
      component.
    autodeploy-verifier-enabled
      To enable/disable verifier, during auto-deployment. If true,
      verification will be done before any deployment activity. In
      the event of any verifier test failure, deployment is not
      performed.
    deploy-xml-validation
      specifies if descriptor validation is required or not.

      full
        xml will be validated and in case of xml validation
        errors, deployment will fail.
      parsing
        xml errors will be reported but deployment process will
        continue.
      none
        no xml validation will be perfomed on the standard or
        runtime deployment descriptors.

    dynamic-reload-enabled
      when true, server checks timestamp on a .reload file at every
      module and application directory level to trigger reload.
      polling frequency is controlled by
      reload-poll-interval-in-seconds

  Used in:
    admin-service
-->
<!ELEMENT das-config (property*)>

<!ATTLIST das-config
    dynamic-reload-enabled %boolean; "false"
    dynamic-reload-poll-interval-in-seconds CDATA "2"
    autodeploy-enabled %boolean; "false"
    autodeploy-polling-interval-in-seconds CDATA "2"
    autodeploy-dir CDATA "autodeploy"
```

```
    autodeploy-verifier-enabled %boolean; "false"
    autodeploy-jsp-precompilation-enabled %boolean; "false"
    deploy-xml-validation %validation-level; "full"
    admin-session-timeout-in-minutes CDATA "60">


<!-- web-container

  Used in:
    config
-->
<!ELEMENT web-container (session-config?, property*)>


<!-- session-config

  Used in:
    web-container
-->
<!ELEMENT session-config (session-manager?, session-properties?)>


<!-- session-manager

  Used in:
    session-config
-->
<!ELEMENT session-manager (manager-properties?, store-properties?)>


<!-- manager-properties

  Used in:
    session-manager
-->
<!ELEMENT manager-properties (property*)>

<!ATTLIST manager-properties
    session-file-name CDATA #IMPLIED
    reap-interval-in-seconds CDATA #IMPLIED
    max-sessions CDATA #IMPLIED
```

```
    session-id-generator-classname CDATA #IMPLIED>


<!-- store-properties

  Used in:
    session-manager
-->
<!ELEMENT store-properties (property*)>

<!ATTLIST store-properties
    directory CDATA #IMPLIED
    reap-interval-in-seconds CDATA #IMPLIED>


<!-- session-properties

  Used in:
    session-config
-->
<!ELEMENT session-properties (property*)>

<!ATTLIST session-properties
    timeout-in-seconds CDATA #IMPLIED>


<!-- ejb-container
    Configuration of EJB Container.

  children
    ejb-timer-service
        The ejb-timer-service element contains the configuration for
        the ejb timer service. There is at most one ejb timer service
        per server instance.

  attributes
    cache-idle-timeout-in-seconds
        (eb, sfsb) specifies the rate at which the cache cleaner
        thread is scheduled. All idle instances are passivated at
        once.
    cache-resize-quantity
```

(eb,sfsb) Cache elements have identity, hence growth is in unit steps and created on demand. Shrinking of cache happens

when cache-idle-timeout-in-seconds timer expires and a cleaner thread passivates beans which have been idle for longer than cache-idle-timeout-in-seconds. All idle instances are passivated at once. cache-resize-quantity does not apply in this case.

when max cache size is reached, an asynchronous task is created to bring the size back under the max-cache-size limit. This task removes cache-resize-quantity elements, consulting the victim-selection-policy.

Must be greater than 1 and less than max-cache-size.

commit-option
(eb) Entity Beans caching is controlled by this setting. Commit Option C implies that no caching is performed in the container.

max-cache-size
(sfsb,eb) specifies the maximum number of instances that can be cached. For entity beans, internally two caches are maintained for higher concurrency: (i) Ready (R$) (ii) Active in an Incomplete Transaction (TX$). The TX$ is populated with instances from R$ or from the Pool directly. When an instance in TX$ completes the transaction, it is placed back in the R$ (or in pool, in case an instance with same identity already is in R$). max-cache-size only specifies the upper limit for R$. The container computes an appropriate size for TX$. For SFSBs, after the max-cache-size is reached, beans (as determined by the victim-selection-policy) get passivated.

max-pool-size
(slsb,eb) maximum size, a pool can grow to. A value of 0 implies an unbounded pool. Unbounded pools eventually shrink to the steady-pool-size, in steps defined by pool-resize-quantity.

pool-idle-timeout-in-seconds
(slsb,eb) defines the rate at which the pool cleaning thread is executed. this thread checks if current size is greater than steady pool size, it removes pool-resize-quantity elements. If the current size is less than steady-pool-size it is increased by pool-resize-quantity, with a ceiling of

min (current-pool-size + pool-resize-quantity, max-pool-size)
Only objects that have not been accessed for more than pool-idle-timeout-in-seconds are candidates for removal.

pool-resize-quantity
(slsb,eb) size of bean pool grows (shrinks) in steps specified by pool-resize-quantity, subject to max-pool-size (steady-pool-size) limit.

removal-timeout-in-seconds
(sfsb) Instance is removed from cache or passivation store, if it is not accesed within this time. All instances that can be removed, will be removed.

session-store
specifies the directory where passivated beans and persisted HTTP sessions are stored on the file system. Defaults to $INSTANCE-ROOT/session-store

steady-pool-size
(slsb,eb) number of bean instances normally maintained in pool. When a pool is first created, it will be populated with size equal to steady-pool-size. When an instance is removed from the pool, it is replenished asynchronously, so that the pool size is at or above the steady-pool-size. This additions will be in multiples of pool-resize-quantity. When a bean is disassociated from a method invocation, it is put back in the pool, subject to max-pool-size limit. If the max pool size is exceeded the bean id destroyed immediately. A pool cleaning thread, executes at an interval defined by pool-idle-timeout-in-seconds. This thread reduces the pool size to steady-pool-size, in steps defined by pool-resize-quantity. If the pool is empty, the required object will be created and returned immediately. This prevents threads from blocking till the pool is replenished by the background thread. steady-pool-size must be greater than 1 and at most equal to the max-pool-size.

victim-selection-policy
(sfsb) Victim selection policy when cache needs to shrink. Victims are passivated. Entity Bean Victims are selected always using fifo discipline. Does not apply to slsb because it does not matter, which particular instances are removed.
fifo
method picks victims, oldest instance first.
lru

```
            algorithm picks least recently accessed instances.
        nru
            policy tries to pick 'not recently used' instances and is
            a pseudo-random selection process.

  Used in:
    config
-->
<!ELEMENT ejb-container (ejb-timer-service?, property*)>

<!ATTLIST ejb-container
    steady-pool-size CDATA "32"
    pool-resize-quantity CDATA "16"
    max-pool-size CDATA "64"
    cache-resize-quantity CDATA "32"
    max-cache-size CDATA "512"
    pool-idle-timeout-in-seconds CDATA "600"
    cache-idle-timeout-in-seconds CDATA "600"
    removal-timeout-in-seconds CDATA "5400"
    victim-selection-policy (fifo | lru | nru) "nru"
    commit-option (B | C) "B"
    session-store CDATA #IMPLIED>


<!-- ejb-timer-service
    Configuration for ejb timer service.

  attributes
    max-redeliveries
        is the maximum number of times the ejb timer service will
        attempt to redeliver a timer expiration due to exception or
        rollback. The minimum value is 1, per the ejb specification.
    minimum-delivery-interval-in-millis
        is the minimum number of milliseconds allowed before the next
        timer expiration for a particular timer can occur. It guards
        against extremely small timer increments that can overload
        the server.
    redelivery-interval-internal-in-millis
        is the number of milliseconds the ejb timer service will wait
        after a failed ejbTimeout delivery before attempting a
        redelivery.
```

```
    timer-datasource
        overrides the cmp-resource (jdbc/__TimerPool) specified in
        sun-ejb-jar.xml of (__ejb_container_timer_app) of the timer
        service system application. By default this is set to
        jdbc/__TimerPool, but can be overridden for the cluster or
        server instance, if they choose to.

  Used in:
    ejb-container
-->
<!ELEMENT ejb-timer-service (property*)>

<!ATTLIST ejb-timer-service
    minimum-delivery-interval-in-millis CDATA "7000"
    max-redeliveries CDATA "1"
    timer-datasource CDATA #IMPLIED
    redelivery-interval-internal-in-millis CDATA "5000">



<!-- mdb-container

  attributes
    idle-timeout-in-seconds
        idle bean instance in pool becomes a candidate for deletion,
        when this timeout expires.
    max-pool-size
        maximum size, pool can grow to. A non-negative integer.
    pool-resize-quantity
        quantum of increase/decrease, when the size of pool
        grows/shrinks. An integer in the range [0, max-pool-size].
    steady-pool-size
        minimum and initial number of message driven beans in pool.
        An integer in the range [0, max-pool-size].

  Used in:
    config
-->
<!ELEMENT mdb-container (property*)>

<!ATTLIST mdb-container
    steady-pool-size CDATA "10"
```

pool-resize-quantity CDATA "2"
max-pool-size CDATA "60"
idle-timeout-in-seconds CDATA "600">

<!-- jms-service
The jms-service element specifies information about the bundled/built-in JMS service that is managed by Application Server.

attributes
addresslist-behavior
Determines broker selection from imqAddressList.
random
causes selection to be performed randomly
priority
causes selection to be performed sequentially
addresslist-iterations
Number of times reconnect logic should iterate imqAddressList. This property will not be used if the addresslist-behavior is "random". An integer.
default-jms-host
reference to a jms-host that to be started when type of jms-service is LOCAL.
init-timeout-in-seconds
specifies the time server instance will wait at start up, for its corresponding JMS service instance to respond. If there is no response within the specifies timeout period, application server startup is aborted. Default value of 60 seconds.
mq-scheme
Scheme for establishing connection with broker. For example, scheme can be specified as "http" for connecting to MQ broker over http. Default is "mq".
mq-service
Type of broker service. If a broker supports ssl, then the type of service can be "ssljms". If nothing is specified, MQ will assume 4that service is "jms".
reconnect-attempts
Total number of attempts to reconnect. An integer.
reconnect-enabled

Causes reconnect feature to be enabled (true) or disabled (false). A boolean.

reconnect-interval-in-seconds

Interval between reconnect attempts, in seconds. An integer.

start-args

specifies the arguments that will be supplied to start up the corresponding JMS service instance.

type

Type of JMS service.

Used in:

config

-->

```
<!ELEMENT jms-service (jms-host*, property*)>

<!ATTLIST jms-service
   init-timeout-in-seconds CDATA "60"
   type (LOCAL | EMBEDDED | REMOTE) #REQUIRED
   start-args CDATA #IMPLIED
   default-jms-host CDATA #IMPLIED
   reconnect-interval-in-seconds CDATA "5"
   reconnect-attempts CDATA "3"
   reconnect-enabled %boolean; "true"
   addresslist-behavior (random | priority) "random"
   addresslist-iterations CDATA "3"
   mq-scheme CDATA #IMPLIED
   mq-service CDATA #IMPLIED>


<!-- jms-host
```

attributes

admin-password

attribute specifies the admin password.

admin-user-name

specifies the admin username.

host

ip V6 or V4 address or hostname.

port

the port number used by the JMS service.

```
  Used in:
    jms-service
-->
<!ELEMENT jms-host (property*)>

<!ATTLIST jms-host
    name CDATA #REQUIRED
    host CDATA #IMPLIED
    port CDATA "7676"
    admin-user-name CDATA "admin"
    admin-password CDATA "admin">


<!-- log-service
    By default, logs would be kept in $INSTANCE-ROOT/logs. The
    following log files will be stored under the logs directory.

    access.log
        keeps default virtual server HTTP access messages.
    server.log
        keeps log messages from default virtual server. Messages from
        other configured virtual servers also go here, unless
        log-file is explicitly specified in the virtual-server
        element.


  attributes
    alarms
        if true, will turn on alarms for the logger. The SEVERE and
        WARNING messages can be routed through the JMX framework to
        raise SEVERE and WARNING alerts. Alarms are turned off by
        default.
    file
        can be used to rename or relocate server.log using absolute
        path.
    log-filter
        Can plug in a log filter to do custom filtering of log
        records . By default there is no log filter other than the
        log level filtering provided by JSR 047 log API.
    log-handler
        Can plug in a custom log handler to add it to the chain of
```

handlers to log into a different log destination than the default ones given by the system (which are Console, File and Syslog). It is a requirement that customers use the log formatter provided by the the system to maintain uniformity in log messages. The custom log handler will be added at the end of the handler chain after File + Syslog Handler, Console Handler and JMX Handler. User cannot replace the handler provided by the system, because of loosing precious log statements. The Server Initialization will take care of installing the custom handler with the system formatter initialized. The user need to use JSR 047 Log Handler Interface to implement the custom handler.

log-rotation-limit-in-bytes
Log Files will be rotated when the file size reaches the limit.

log-rotation-timelimit-in-minutes
This is a new attribute to enable time based log rotation. The Log File will be rotated only if this value is non-zero and the valid range is 60 minutes (1 hour) to 10*24*60 minutes (10 days). If the value is zero then the files will be rotated based on size specified in log-rotation-limit-in-bytes.

log-to-console
logs will be sent to stderr when asadmin start-domain verbose is used

retain-error-statistics-for-hours
The number of hours since server start, for which error statistics should be retained in memory. The default and minimum value is 5 hours. The maximum value allowed is 500 hours. Note that larger values will incur additional memory overhead.

use-system-logging
if true, will utilize Unix syslog service or Windows Event Logging to produce and manage logs.

Used in:
config, node-agent
-->
<!ELEMENT log-service (module-log-levels?, property*)>

<!ATTLIST log-service

```
    file CDATA #IMPLIED
    use-system-logging %boolean; "false"
    log-handler CDATA #IMPLIED
    log-filter CDATA #IMPLIED
    log-to-console %boolean; "false"
    log-rotation-limit-in-bytes CDATA "500000"
    log-rotation-timelimit-in-minutes CDATA "0"
    alarms %boolean; "false"
    retain-error-statistics-for-hours CDATA "5">


<!-- module-log-levels

  Used in:
    log-service
-->
<!ELEMENT module-log-levels (property*)>

<!ATTLIST module-log-levels
    root %log-level; "INFO"
    server %log-level; "INFO"
    ejb-container %log-level; "INFO"
    cmp-container %log-level; "INFO"
    mdb-container %log-level; "INFO"
    web-container %log-level; "INFO"
    classloader %log-level; "INFO"
    configuration %log-level; "INFO"
    naming %log-level; "INFO"
    security %log-level; "INFO"
    jts %log-level; "INFO"
    jta %log-level; "INFO"
    admin %log-level; "INFO"
    deployment %log-level; "INFO"
    verifier %log-level; "INFO"
    jaxr %log-level; "INFO"
    jaxrpc %log-level; "INFO"
    saaj %log-level; "INFO"
    corba %log-level; "INFO"
    javamail %log-level; "INFO"
    jms %log-level; "INFO"
    connector %log-level; "INFO"
```

```
    jdo %log-level; "INFO"
    cmp %log-level; "INFO"
    util %log-level; "INFO"
    resource-adapter %log-level; "INFO"
    synchronization %log-level; "INFO"
    node-agent %log-level; "INFO"
    self-management %log-level; "INFO"
    group-management-service %log-level; "INFO"
    management-event %log-level; "INFO">


<!-- security-service
    The security service element defines parameters and configuration
    information needed by the core J2EE security service. Some
    container-specific security configuration elements are in the
    various container configuration elements and not here. SSL
    configuration is also elsewhere. At this time the security
    service configuration consists of a set of authentication realms.
    A number of top-level attributes are defined as well.

  children
    message-security-config
        Optional list of layer specific lists of configured message
        security providers.

  attributes
    activate-default-principal-to-role-mapping
        Causes the appserver to apply a default principal to role
        mapping, to any application that does not have an application
        specific mapping defined. Every role is mapped to a
        same-named (as the role) instance of a
        java.security.Principal implementation class (see
        mapped-principal-class). This behavior is similar to that of
        Tomcat servlet container. It is off by default.
    anonymous-role
        This attribute is deprecated.
    audit-enabled
        If true, additional access logging is performed to provide
        audit information.
    audit-modules
        Optional list of audit provider modules which will be used by
```

```
      the audit subsystem. The default value refers to the internal
      log-based audit module.
    default-principal
      Used as the identity of default security contexts when
      necessary and no principal is provided.
    default-principal-password
      Password of default principal.
    default-realm
      Specifies which realm (by name) is used by default when no
      realm is specifically requested. The file realm is the common
      default.
    jacc
      Specifies the name of the jacc-provider element to use for
      setting up the JACC infrastructure. The default value
      "default" does not need to be changed unless adding a custom
      JACC provider.
    mapped-principal-class
      This attribute is used to customize the
      java.security.Principal implementation class used in the
      default principal to role mapping. This attribute is
      optional. When it is not specified,
      com.sun.enterprise.deployment.Group implementation of
      java.security.Principal is used. The value of this attribute
      is only relevant when the activate-default
      principal-to-role-mapping attribute is set to true.

  Used in:
    config
-->
<!ELEMENT security-service
    (auth-realm+, jacc-provider+, audit-module*, message-security-config*,
    property*)>


<!ATTLIST security-service
    default-realm CDATA "file"
    default-principal CDATA #IMPLIED
    default-principal-password CDATA #IMPLIED
    anonymous-role CDATA "AttributeDeprecated"
    audit-enabled %boolean; "false"
    jacc CDATA "default"
```

```
    audit-modules CDATA "default"
    activate-default-principal-to-role-mapping %boolean; "false"
    mapped-principal-class CDATA #IMPLIED>


<!-- audit-module
    An audit-module specifies an optional plug-in module which
    implements audit capabilities.

  attributes
    classname
        defines the java class which implements this audit module
    name
        defines the name of this realm

  Used in:
    security-service
-->
<!ELEMENT audit-module (property*)>

<!ATTLIST audit-module
    name CDATA #REQUIRED
    classname CDATA #REQUIRED>


<!-- auth-realm
    The auth-realm element defines and configures one authentication
    realm. There must be at least one realm available for a server
    instance; any number can be configured, as desired.

    Authentication realms need provider-specific parameters which vary
    depending on what a particular implementation needs; these are defined as
    properties since they vary by provider and cannot be predicted for any
    custom or add-on providers.

    For the default file provider, the param used is: file


  attributes
    classname
        defines the java class which implements this realm
```

```
    name
        defines the name of this realm

  Used in:
    node-agent, security-service
-->
<!ELEMENT auth-realm (property*)>

<!ATTLIST auth-realm
    name CDATA #REQUIRED
    classname CDATA #REQUIRED>


<!-- jacc-provider
    The jacc-provider element defines the standard JACC properties
    used for setting up the JACC provider. It also allows optional
    properties which can be used by the provider implementation for
    its configuration.

  attributes
    name
        A name for this jacc-provider. Is always "default" for the
        default provider.
    policy-configuration-factory-provider
        Corresponds to (and can be overridden by) the system property
        javax.security.jacc.PolicyConfigurationFactory.provider
    policy-provider
        Corresponds to (and can be overridden by) the system property
        javax.security.jacc.policy.provider

  Used in:
    security-service
-->
<!ELEMENT jacc-provider (property*)>

<!ATTLIST jacc-provider
    name CDATA #REQUIRED
    policy-provider CDATA #REQUIRED
    policy-configuration-factory-provider CDATA #REQUIRED>
```

<!-- transaction-service
Configuration for Transaction Manager.

attributes
automatic-recovery
if true, server instance attempts recovery at restart.
heuristic-decision
During recovery, if outcome of a transaction cannot be determined from the logs, then this property is used to fix the outcome.
keypoint-interval
property used to specify the number of transactions between keypoint operations on the log. A Keypoint operations could reduce the size of the transaction log files. A larger value for this property (for example, 1000) will result in larger transaction log files, between log compactions, but less keypoint operations, and potentially better performance. A smaller value (e.g. 20) results in smaller log files but slightly reduced performance due to the greater frequency of keypoint operations.
retry-timeout-in-seconds
used to determine the retry time in the following scenarios.

1 Time to wait at the transaction recovery time, when resources are unreachable.
2 If there are any transient exceptions in the second phase of the 2 PC protocol.

A negative value indicates infinite retry. '0' indicates no retry. A positive value indicates the number of seconds for which retry will be attempted. Default is 10 minutes which may be appropriate for a database being restarted.
timeout-in-seconds
amount of time the transaction manager waits for response from a datasource participating in transaction. A value of 0 implies infinite timeout.
tx-log-dir
Transaction service creates a sub directory 'tx' under tx-log-dir to store the transaction logs. The default value of the tx-log-dir is $INSTANCE-ROOT/logs. If this attribute is not explicitly specified in the <transaction-service>

```
        element, 'tx' sub directory will be created under the path
        specified in log-root attribute of <domain> element.

  Used in:
    config
-->
<!ELEMENT transaction-service (property*)>

<!ATTLIST transaction-service
    automatic-recovery %boolean; "false"
    timeout-in-seconds CDATA "0"
    tx-log-dir CDATA #IMPLIED
    heuristic-decision (rollback | commit) "rollback"
    retry-timeout-in-seconds CDATA "600"
    keypoint-interval CDATA "2048">


<!-- monitoring-service

  Used in:
    config
-->
<!ELEMENT monitoring-service (module-monitoring-levels?, property*)>


<!-- module-monitoring-levels

  attributes
    connector-connection-pool
        monitoring level for all the connector-connection-pools used
        by the runtime.
    ejb-container
        various ejbs deployed to the server, ejb-pools, ejb-caches
        and ejb-methods.
    http-service
        http engine and the http listeners therein.
    jdbc-connection-pool
        monitoring level for all the jdbc-connection-pools used by
        the runtime.
    orb
        specifies the level for connection managers of the orb, which
```

```
        apply to connections to the orb
    thread-pool
        all the thread-pools used by the run time.
    transaction-service
        transaction subsystem.

  Used in:
    monitoring-service
-->
<!ELEMENT module-monitoring-levels (property*)>

<!ATTLIST module-monitoring-levels
    thread-pool %monitoring-level; "OFF"
    orb %monitoring-level; "OFF"
    ejb-container %monitoring-level; "OFF"
    web-container %monitoring-level; "OFF"
    transaction-service %monitoring-level; "OFF"
    http-service %monitoring-level; "OFF"
    jdbc-connection-pool %monitoring-level; "OFF"
    connector-connection-pool %monitoring-level; "OFF"
    connector-service %monitoring-level; "OFF"
    jms-service %monitoring-level; "OFF"
    jvm %monitoring-level; "OFF">


<!-- diagnostic-service

  attributes
    capture-app-dd
        boolean attribute. If "true", application deployment
        descriptors in plain text are captured as part of diagnostic
        report. If Deployment descriptors contain any confidential
        information, it's recommended to set it to false.
    capture-hadb-info
        boolean attribute to indicate whether HADB related
        information is collected.
    capture-install-log
        boolean attribute which indicated whether the log generated
        during installation of the application server is captured.
    capture-system-info
        boolean attribute which specifies whether OS level
```

information is collected as part of diagnostic report.
compute-checksum
boolean attribute. Indicates whether checksum of binaries is computed.
max-log-entries
Max no. of log entries being captured as part of diagnostic report. A non negative value.
min-log-level
The log levels can be changed using one of the seven levels. Please refer JSR 047 to understand the Log Levels. The default level is INFO, meaning that messages at that level or higher (WARNING, SEVERE) are captured as part of the diagnostic report.If set to OFF, log contents will not be captured as part of diagnostic report.
verify-config
A boolean attribute which indicates whether output of verify-config asadmin command is included in the diagnostic report.

Used in:
config
-->
<!ELEMENT diagnostic-service (property*)>

<!ATTLIST diagnostic-service
compute-checksum %boolean; "true"
verify-config %boolean; "true"
capture-install-log %boolean; "true"
capture-system-info %boolean; "true"
capture-hadb-info %boolean; "true"
capture-app-dd %boolean; "true"
min-log-level %log-level; "INFO"
max-log-entries CDATA "500">

<!-- group-management-service
group-management-service(GMS) is an in-process service that provides cluster monitoring and group communication services. GMS notifies registered modules in an application server instance when one or more members in the cluster fail (become unreachable). GMS also provides the ability to send and receive

```
    messages between a group of processes. GMS is a abstraction layer
    that plugs-in group communication technologies which rely on a
    configurable stack of protocols. Each of these protocols has
    properties that can be changed for a given network and deployment
    topology. These relevant configurable protocols are: fd-protocol
    enables its members to periodically monitor other group members
    to determine their availability in the group. merge-protocol is
    used to reunite subgroups that formed as a result of a network
    partition after such a partition has healed. ping-protocol is
    used for discovery of the group and its members. vs-protocol
    verifies suspect instances by adding a verification layer to mark
    a failure suspicion as a confirmed failure.

  attributes
    fd-protocol-max-tries
        Maximum number of attempts to try before GMS confirms that a
        failure is suspected in the group. Must be a positive integer.
    fd-protocol-timeout-in-millis
        Period of time between monitoring attempts to detect failure.
        Must be a positive integer.
    merge-protocol-max-interval-in-millis
        Specifies the maximum amount of time to wait to collect
        sub-group information before performing a merge. Must be a
        positive integer.
    merge-protocol-min-interval-in-millis
        specifies the minimum amount of time to wait to collect
        sub-group information before performing a merge. Must be a
        positive integer.
    ping-protocol-timeout-in-millis
        Amount of time in milliseconds that GMS waits for discovery
        of other members in this group. Must be a positive integer.
    vs-protocol-timeout-in-millis
        After this timeout a suspected failure is marked as verified.
        Must be a positive integer.

  Used in:
    config
-->
<!ELEMENT group-management-service (property*)>

<!ATTLIST group-management-service
```

```
    fd-protocol-max-tries CDATA "3"
    fd-protocol-timeout-in-millis CDATA "2000"
    merge-protocol-max-interval-in-millis CDATA "10000"
    merge-protocol-min-interval-in-millis CDATA "5000"
    ping-protocol-timeout-in-millis CDATA "2000"
    vs-protocol-timeout-in-millis CDATA "1500">


<!-- java-config
    Java Runtime environment configuration

  attributes
    bytecode-preprocessors
        A comma separated list of classnames, each of which must
        implement the com.sun.appserv.BytecodePreprocessor interface.
        Each of the specified preprocessor class will be called in
        the order specified. At the moment the comelling use is for a
        3rd party Performance Profiling tool.
    classpath-prefix
        A java classpath string that is prefixed to server-classpath
    classpath-suffix
        A java classpath string that is appended to server-classpath
    debug-enabled
        If set to true, the server starts up in debug mode ready for
        attaching with a JPDA based debugger.
    debug-options
        JPDA based debugging options string.
    env-classpath-ignored
        If set to false, the CLASSPATH environment variable will be
        read and appended to the Application Server classpath, which
        is constructed as described above. The CLASSPATH environment
        variable will be added after the classpath-suffix, at the
        very end.
    javac-options
        Options string passed to Java compiler, at application
        deployment time.
    java-home
        Specifies the installation directory for Java runtime. JDK
        1.4 or higher is supported.
    native-library-path-prefix
        is prepended to the native library path, which is constructed
```

```
        internally.

        Internally, the native library path is automatically constructed to be
        a concatenation of 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.

    native-library-path-suffix
        is appended to the native library path, which is constructed
        as described above.
    rmic-options
        Options string passed to RMI compiler, at application
        deployment time.
    server-classpath
        A java classpath string that specifies the classes needed by
        the Application server. Do not expect users to change this
        under normal conditions. The shared application server
        classloader forms the final classpath by concatenating
        classpath-prefix, ${INSTALL_DIR}/lib, server-classpath, and
        classpath-suffix.
    system-classpath
        This classpath string supplied to the jvm at server startup.
        Contains appserv-launch.jar by default. Users may add to this
        classpath.

  Used in:
    config
-->
<!ELEMENT java-config (profiler?, (jvm-options | property)*)>

<!ATTLIST java-config
    java-home CDATA "${com.sun.aas.javaRoot}"
    debug-enabled %boolean; "false"
    debug-options CDATA "-Xdebug -
Xrunjdwp:transport=dt_socket,server=y,suspend=n"
    rmic-options CDATA "-iiop -poa -alwaysgenerate -keepgenerated -g"
    javac-options CDATA "-g"
    classpath-prefix CDATA #IMPLIED
    classpath-suffix CDATA #IMPLIED
    server-classpath CDATA #IMPLIED
```

```
    system-classpath CDATA #IMPLIED
    native-library-path-prefix CDATA #IMPLIED
    native-library-path-suffix CDATA #IMPLIED
    bytecode-preprocessors CDATA #IMPLIED
    env-classpath-ignored %boolean; "true">


<!-- jvm-options
    String value for options that will be passed to the JVM

  Used in:
    java-config, profiler
-->
<!ELEMENT jvm-options (#PCDATA)>


<!-- profiler
    Profilers could be one of jprobe, optimizeit, hprof, wily and so
    on jvm-options and property elements are used to record the
    settings needed to get a particular profiler going. A server
    instance is tied to a particular profiler, by the profiler
    element in java-config. Changing the profiler will require a
    server restart.

    The adminstrative graphical interfaces, could list multiple supported
    profilers (incomplete at this point) and will populate server.xml
    appropriately.


  Used in:
    java-config
-->
<!ELEMENT profiler ((jvm-options | property)*)>

<!ATTLIST profiler
    name CDATA #REQUIRED
    classpath CDATA #IMPLIED
    native-library-path CDATA #IMPLIED
    enabled %boolean; "true">
```

<!-- availability-service
SE/EE only: TBD Needs explanation

attributes
auto-manage-ha-store
If set to true, the lifecycle of the highly available store is matched with the lifecycle of the highly available cluster. The store is started or stopped with the cluster. It is removed when the cluster is deleted. When set to false, the store lifecycle would have to manually managed by the administrator.
ha-agent-hosts
comma-delimited list of server host names or IP addresses where high availability store management agents are running.
ha-agent-password
password needed to contact highly available store management agents
ha-agent-port
port number where highly available store management agents can be contacted
ha-store-healthcheck-enabled
Application server stops saving session state when the store service does not function properly or is is not accessible for any reason. When this attribute is set to true, periodic checking is done to detect if the store service has become available again. If healthcheck succeeds the session state saving is resumed. Defaults to false.
ha-store-healthcheck-interval-in-seconds
The periodicity at which store health is checked.
ha-store-name
Name of the session store
store-pool-name
This is the jndi-name for the JDBC Connection Pool used potentially by both the Web Container and the EJB Stateful Session Bean Container for use in checkpointing/passivation when persistence-type = "ha". See sfsb-ha-persistence-type and sfsb-persistence-type for more details. It will default to "jdbc/hastore". This attribute can be over-ridden in either web-container-availability (with http-session-store-pool-name) and/or in ejb-container-availability (with sfsb-store-pool-name). If

```
        store-pool-name is not over-ridden then both containers will
        share the same connection pool. If either container
        over-rides then it may have its own dedicated pool. In this
        case there must also be a new corresponding JDBC Resource and
        JDBC Connection Pool defined for this new pool name.

      Used in:
        config
-->
<!ELEMENT availability-service
    (web-container-availability?, ejb-container-availability?,
    jms-availability?, property*)>


<!ATTLIST availability-service
    availability-enabled %boolean; "true"
    ha-agent-hosts CDATA #IMPLIED
    ha-agent-port CDATA #IMPLIED
    ha-agent-password CDATA #IMPLIED
    ha-store-name CDATA #IMPLIED
    auto-manage-ha-store %boolean; "false"
    store-pool-name CDATA #IMPLIED
    ha-store-healthcheck-enabled %boolean; "false"
    ha-store-healthcheck-interval-in-seconds CDATA "5">


<!-- web-container-availability
    web-container-availability SE/EE only:

      attributes
        availability-enabled
            This boolean flag controls whether availability is enabled
            for HTTP session persistence. If this is "false", then
            session persistence is disabled for all web modules in j2ee
            apps and stand-alone web modules. If it is "true" (and
            providing that the global availability-enabled in
            availability-service is also "true", then j2ee apps and
            stand-alone web modules may be ha enabled. Finer-grained
            control exists at lower levels. If this attribute is missing,
            it "inherits" the value of the global availability-enabled
            under availability-service.
```

```
    http-session-store-pool-name
        This is the jndi-name for the JDBC Connection Pool used by
        the HTTP Session Persistence Framework. If missing, internal
        code will default it to value of store-pool-name under
        availability-service (ultimately "jdbc/hastore").
    persistence-frequency
        The persistence frequency used by the session persistence
        framework, when persistence-type = "ha". Values may be
        "time-based" or "web-event". If it is missing, then the
        persistence-type will revert to "memory".
    persistence-scope
        The persistence scope used by the session persistence
        framework, when persistence-type = "ha". Values may be
        "session", "modified-session", "modified-attribute". If it is
        missing, then the persistence-type will revert to "memory".
    persistence-store-health-check-enabled
        Deprecated. This attribute has no effect. If you wish to
        control enabling/disabling HADB health check, refer to
        store-healthcheck-enabled attribute in the
        availability-service element.
    persistence-type
        Specifies the session persistence mechanism for web
        applications that have availability enabled. Default is
        "memory".
    sso-failover-enabled
        This controls whether Single-Sign-On state will be made
        available for failover.

  Used in:
    availability-service
-->
<!ELEMENT web-container-availability (property*)>

<!ATTLIST web-container-availability
    availability-enabled %boolean; #IMPLIED
    persistence-type CDATA "memory"
    persistence-frequency %session-save-frequency; #IMPLIED
    persistence-scope %session-save-scope; #IMPLIED
    persistence-store-health-check-enabled %boolean; "false"
    sso-failover-enabled %boolean; "false"
    http-session-store-pool-name CDATA #IMPLIED>
```

```
<!-- ejb-container-availability

  attributes
    availability-enabled
        This boolean flag controls whether availability is enabled
        for SFSB checkpointing (and potentially passivation). If this
        is "false", then all SFSB checkpointing is disabled for all
        j2ee apps and ejb modules. If it is "true" (and providing
        that the global availability-enabled in availability-service
        is also "true", then j2ee apps and stand-alone ejb modules
        may be ha enabled. Finer-grained control exists at lower
        levels. If this attribute is missing, it inherits the value
        of the global availability-enabled under availability-service.
    sfsb-checkpoint-enabled
        This attribute is deprecated, replaced by
        availability-enabled and will be ignored if present.
    sfsb-ha-persistence-type
        The persistence type used by the EJB Stateful Session Bean
        Container for checkpointing and passivating
        availability-enabled beans' state. Default is "ha".
    sfsb-persistence-type
        Specifies the passivation mechanism for stateful session
        beans that do not have availability enabled. Default is
        "file".
    sfsb-quick-checkpoint-enabled
        This attribute is deprecated and will be ignored if present.
    sfsb-store-pool-name
        This is the jndi-name for the JDBC Connection Pool used by
        the EJB Stateful Session Bean Container for use in
        checkpointing/passivation when persistence-type = "ha". See
        sfsb-ha-persistence-type and sfsb-persistence-type for more
        details. It will default to value of store-pool-name under
        availability-service (ultimately "jdbc/hastore").

  Used in:
    availability-service
-->
<!ELEMENT ejb-container-availability (property*)>
```

<!ATTLIST ejb-container-availability
availability-enabled %boolean; #IMPLIED
sfsb-ha-persistence-type CDATA "ha"
sfsb-persistence-type CDATA "file"
sfsb-checkpoint-enabled %boolean; #IMPLIED
sfsb-quick-checkpoint-enabled %boolean; #IMPLIED
sfsb-store-pool-name CDATA #IMPLIED>

<!-- jdbc-connection-pool
jdbc-connection-pool defines configuration used to create and manage a pool physical database connections. Pool definition is named, and can be referred to by multiple jdbc-resource elements (See <jdbc-resource>).

Each named pool definition results in a pool instantiated at server start-up. Pool is populated when accessed for the first time. If two or more jdbc-resource elements point to the same jdbc-connection-pool element, they are using the same pool of connections, at run time.

children
property
Most JDBC 2.0 drivers permit use of standard property lists, to specify User, Password and other resource configuration. While these are optional properties, according to the specification, several of these properties may be necessary for most databases. See Section 5.3 of JDBC 2.0 Standard Extension API.

The following are the names and corresponding values for these properties

databaseName
Name of the Database
serverName
Database Server name.
port
Port where a Database server is listening for requests.
networkProtocol
Communication Protocol used.

user
default name of the database user with which connections will be stablished. Programmatic database authentication or default-resource-principal specified in vendor specific web and ejb deployment descriptors will take precedence, over this default. The details and caveats are described in detail in the Administrator's guide.
password
password for default database user
roleName
The initial SQL role name.
datasourceName
used to name an underlying XADataSource, or ConnectionPoolDataSource when pooling of connections is done
description
Textual Description

When one or more of these properties are specified, they are passed as is using set<Name>(<Value>) methods to the vendors Datasource class (specified in datasource-classname). User and Password properties are used as default principal, if Container Managed authentication is specified and a default-resource-principal is not found in application deployment descriptors.

attributes
allow-non-component-callers
A pool with this property set to true, can be used by non-J2EE components (i.e components other than EJBs or Servlets). The returned connection is enlisted automatically with the transaction context obtained from the transaction manager. This property is to enable the pool to be used by non-component callers such as ServletFilters, Lifecycle modules, and 3rd party persistence managers. Standard J2EE components can continue to use such pools. Connections obtained by non-component callers are not automatically cleaned at the end of a transaction by the container. They need to be explicitly closed by the the caller.
associate-with-thread
Associate a connection with the thread such that when the

same thread is in need of a connection, it can reuse the connection already associated with that thread, thereby not incurring the overhead of getting a connection from the pool. Default value is false.

connection-creation-retry-attempts
: The number of attempts to create a new connection. Default is 0, which implies no retries.

connection-creation-retry-interval-in-seconds
: The time interval between retries while attempting to create a connection. Default is 10 seconds. Effective when connection-creation-retry-attempts is greater than 0.

connection-leak-reclaim
: If enabled, connection will be reusable (put back into pool) after connection-leak-timeout-in-seconds occurs. Default value is false.

connection-leak-timeout-in-seconds
: To aid user in detecting potential connection leaks by the application. When a connection is not returned back to the pool by the application within the specified period, it is assumed to be a potential leak and stack trace of the caller will be logged. Default is 0, which implies there is no leak detection, by default. A positive non-zero value turns on leak detection. Note however that, this attribute only detects if there is a connection leak. The connection can be reclaimed only if connection-leak-reclaim is set to true.

connection-validation-method
: specifies the type of validation to be performed when is-connection-validation-required is true. The following types of validation are supported:

  auto-commit
  : using connection.autoCommit()

  meta-data
  : using connection.getMetaData()

  table
  : performing a query on a user specified table (see validation-table-name).

datasource-classname
: Name of the vendor supplied JDBC datasource resource manager. An XA or global transactions capable datasource class will implement javax.sql.XADatasource interface. Non XA or Local transactions only datasources will implement

javax.sql.Datasource interface.

fail-all-connections

indicates if all connections in the pool must be closed should a single validation check fail. The default is false. One attempt will be made to re-establish failed connections.

idle-timeout-in-seconds

maximum time in seconds, that a connection can remain idle in the pool. After this time, the pool implementation can close this connection. Note that this does not control connection timeouts enforced at the database server side. Adminsitrators are advised to keep this timeout shorter than the database server side timeout (if such timeouts are configured on the specific vendor's database), to prevent accumulation of unusable connection in Application Server.

is-connection-validation-required

if true, connections are validated (checked to find out if they are usable) before giving out to the application. The default is false.

is-isolation-level-guaranteed

Applicable only when a particular isolation level is specified for transaction-isolation-level. The default value is true. This assures that every time a connection is obtained from the pool, it is guaranteed to have the isolation set to the desired value. This could have some performance impact on some JDBC drivers. Can be set to false by that administrator when they are certain that the application does not change the isolation level before returning the connection.

lazy-connection-association

Connections are lazily associated when an operation is performed on them. Also, they are disassociated when the transaction is completed and a component method ends, which helps reuse of the physical connections. Default value is false.

lazy-connection-enlistment

Enlist a resource to the transaction only when it is actually used in a method, which avoids enlistment of connections that are not used in a transaction. This also prevents unnecessary enlistment of connections cached in the calling components. Default value is false.

match-connections

To switch on/off connection matching for the pool. It can be set to false if the administrator knows that the connections in the pool will always be homogeneous and hence a connection picked from the pool need not be matched by the resource adapter. Default value is false.

max-connection-usage-count

When specified, connections will be re-used by the pool for the specified number of times after which it will be closed. This is useful for instance, to avoid statement-leaks. Default value is 0, which implies the feature is not enabled.

max-pool-size

maximum number of conections that can be created

max-wait-time-in-millis

amount of time the caller will wait before getting a connection timeout. The default is 60 seconds. A value of 0 will force caller to wait indefinitely.

name

unique name of the pool definition.

non-transactional-connections

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

pool-resize-quantity

number of connections to be removed when idle-timeout-in-seconds timer expires. Connections that have idled for longer than the timeout are candidates for removal. When the pool size reaches steady-pool-size, the connection removal stops.

res-type

DataSource implementation class could implement one of of javax.sql.DataSource, javax.sql.XADataSource or javax.sql.ConnectionPoolDataSource interfaces. This optional attribute must be specified to disambiguate when a Datasource class implements two or more of these interfaces. An error is produced when this attribute has a legal value and the indicated interface is not implemented by the datasource class. This attribute has no default value.

statement-timeout-in-seconds

Sets the timeout property of a connection to enable termination of abnormally long running queries. Default value of -1 implies that it is not enabled.

```
    steady-pool-size
        minimum and initial number of connections maintained in the
        pool.
    transaction-isolation-level
        Specifies the Transaction Isolation Level on the pooled
        database connections. Optional. Has no default. If left
        unspecified the pool operates with default isolation level
        provided by the JDBC Driver. A desired isolation level can be
        set using one of the standard transaction isolation levels,
        which see.

        Applications that change the Isolation level on a pooled connection
        programmatically, risk polluting the pool and this could lead to
        program errors. Also see: is-isolation-level-guaranteed

    validate-atmost-once-period-in-seconds
        Used to set the time-interval within which a connection is
        validated atmost once. Default is 0 which implies that it is
        not enabled. TBD: Documentation is to be corrected.
    validation-table-name
        specifies the table name to be used to perform a query to
        validate a connection. This parameter is mandatory, if
        connection-validation-type set to table. Verification by
        accessing a user specified table may become necessary for
        connection validation, particularly if database driver caches
        calls to setAutoCommit() and getMetaData().
    wrap-jdbc-objects
        When set to true, application will get wrapped jdbc objects
        for Statement, PreparedStatement, CallableStatement,
        ResultSet, DatabaseMetaData. Defaults to false.

  Used in:
    resources
-->
<!ELEMENT jdbc-connection-pool (description?, property*)>

<!ATTLIST jdbc-connection-pool
    name CDATA #REQUIRED
    datasource-classname CDATA #REQUIRED
    res-type (javax.sql.DataSource | javax.sql.XADataSource |
javax.sql.ConnectionPoolDataSource) #IMPLIED
```

```
    steady-pool-size CDATA "8"
    max-pool-size CDATA "32"
    max-wait-time-in-millis CDATA "60000"
    pool-resize-quantity CDATA "2"
    idle-timeout-in-seconds CDATA "300"
    transaction-isolation-level %isolation; #IMPLIED
    is-isolation-level-guaranteed %boolean; "true"
    is-connection-validation-required %boolean; "false"
    connection-validation-method (auto-commit | meta-data | table) "auto-commit"
    validation-table-name CDATA #IMPLIED
    fail-all-connections %boolean; "false"
    non-transactional-connections %boolean; "false"
    allow-non-component-callers %boolean; "false"
    validate-atmost-once-period-in-seconds CDATA "0"
    connection-leak-timeout-in-seconds CDATA "0"
    connection-leak-reclaim %boolean; "false"
    connection-creation-retry-attempts CDATA "0"
    connection-creation-retry-interval-in-seconds CDATA "10"
    statement-timeout-in-seconds CDATA "-1"
    lazy-connection-enlistment %boolean; "false"
    lazy-connection-association %boolean; "false"
    associate-with-thread %boolean; "false"
    match-connections %boolean; "false"
    max-connection-usage-count CDATA "0"
    wrap-jdbc-objects %boolean; "false">


<!-- connector-connection-pool
    connector-connection-pool defines configuration used to create
    and manage a pool of connections to a EIS. Pool definition is
    named, and can be referred to by multiple connector-resource
    elements (See connector-resource).

    Each named pool definition results in a pool instantiated at server
    start-up. Pool is populated when accessed for the first time. If two or
    more connector-resource elements point to the same
    connector-connection-pool element, they are using the same pool of
    connections, at run time.

    There can be more than one pool for one connection-definition in one
    resource-adapter.
```

children
  property
    Properties are used to override the ManagedConnectionFactory
    javabean configuration settings.

    When one or more of these properties are specified, they are passed as
    is using set<Name>(<Value>) methods to the Resource Adapter's
    ManagedConnectionfactory class (specified in ra.xml).

attributes
  associate-with-thread
    Associate a connection with the thread such that when the
    same thread is in need of a connection, it can reuse the
    connection already associated with that thread, thereby not
    incurring the overhead of getting a connection from the pool.
    Default value is false.
  connection-creation-retry-attempts
    The number of attempts to create a new connection. Default is
    0, which implies no retries.
  connection-creation-retry-interval-in-seconds
    The time interval between retries while attempting to create
    a connection. Default is 10 seconds. Effective when
    connection-creation-retry-attempts is greater than 0.
  connection-definition-name
    unique name, identifying one connection-definition in a
    Resource Adapter. Currently this is ConnectionFactory type.
  connection-leak-reclaim
    If enabled, connection will be reusable (put back into pool)
    after connection-leak-timeout-in-seconds occurs. Default
    value is false.
  connection-leak-timeout-in-seconds
    To aid user in detecting potential connection leaks by the
    application. When a connection is not returned back to the
    pool by the application within the specified period, it is
    assumed to be a potential leak and stack trace of the caller
    will be logged. Default is 0, which implies there is no leak
    detection, by default. A positive non-zero value turns on
    leak detection. Note however that, this attribute only

detects if there is a connection leak. The connection can be reclaimed only if connection-leak-reclaim is set to true.

fail-all-connections
: indicates if all connections in the pool must be closed should a single connection fail validation. The default is false. One attempt will be made to re-establish failed connections.

idle-timeout-in-seconds
: maximum time in seconds, that a connection can remain idle in the pool. After this time, the pool implementation can close this connection. Note that this does not control connection timeouts enforced at the database server side. Adminsitrators are advised to keep this timeout shorter than the EIS connection timeout (if such timeouts are configured on the specific EIS), to prevent accumulation of unusable connection in Application Server.

is-connection-validation-required
: This attribute specifies if the connection that is about to be returned is to be validated by the container,

lazy-connection-association
: Connections are lazily associated when an operation is performed on them. Also, they are disassociated when the transaction is completed and a component method ends, which helps reuse of the physical connections. Default value is false.

lazy-connection-enlistment
: Enlist a resource to the transaction only when it is actually used in a method, which avoids enlistment of connections that are not used in a transaction. This also prevents unnecessary enlistment of connections cached in the calling components. Default value is false.

match-connections
: To switch on/off connection matching for the pool. It can be set to false if the administrator knows that the connections in the pool will always be homogeneous and hence a connection picked from the pool need not be matched by the resource adapter. Default value is true.

max-connection-usage-count
: When specified, connections will be re-used by the pool for the specified number of times after which it will be closed. This is useful for instance, to avoid statement-leaks.

Default value is 0, which implies the feature is not enabled.
max-pool-size
maximum number of conections that can be created
max-wait-time-in-millis
amount of time the caller will wait before getting a connection timeout. The default is 60 seconds. A value of 0 will force caller to wait indefinitely.
name
unique name of the pool definition.
pool-resize-quantity
number of connections to be removed when idle-timeout-in-seconds timer expires. Connections that have idled for longer than the timeout are candidates for removal. When the pool size reaches steady-pool-size, the connection removal stops.
resource-adapter-name
This is the name of resource adapter. Name of .rar file is taken as the unique name for the resource adapter.
steady-pool-size
minimum and initial number of connections maintained in the pool.
transaction-support
Indicates the level of transaction support that this pool will have. Possible values are "XATransaction", "LocalTransaction" and "NoTransaction". This attribute will override that transaction support attribute in the Resource Adapter in a downward compatible way, i.e it can support a lower/equal transaction level than specified in the RA, but not a higher level.
validate-atmost-once-period-in-seconds
Used to set the time-interval within which a connection is validated atmost once. Default is 0 which implies that it is not enabled. TBD: Documentation is to be corrected.

Used in:
resources
-->
<!ELEMENT connector-connection-pool (description?, security-map*, property*)>

<!ATTLIST connector-connection-pool
name CDATA #REQUIRED

```
    resource-adapter-name CDATA #REQUIRED
    connection-definition-name CDATA #REQUIRED
    steady-pool-size CDATA "8"
    max-pool-size CDATA "32"
    max-wait-time-in-millis CDATA "60000"
    pool-resize-quantity CDATA "2"
    idle-timeout-in-seconds CDATA "300"
    fail-all-connections %boolean; "false"
    transaction-support (XATransaction | LocalTransaction | NoTransaction) #IMPLIED
    is-connection-validation-required %boolean; "false"
    validate-atmost-once-period-in-seconds CDATA "0"
    connection-leak-timeout-in-seconds CDATA "0"
    connection-leak-reclaim %boolean; "false"
    connection-creation-retry-attempts CDATA "0"
    connection-creation-retry-interval-in-seconds CDATA "10"
    lazy-connection-enlistment %boolean; "false"
    lazy-connection-association %boolean; "false"
    associate-with-thread %boolean; "false"
    match-connections %boolean; "true"
    max-connection-usage-count CDATA "0">


<!-- security-map
    Perform mapping from principal received during Servlet/EJB
    authentication, to credentials accepted by the EIS. This mapping
    is optional.It is possible to map multiple (server) principal to
    the same backend principal.

  Used in:
    connector-connection-pool
-->
<!ELEMENT security-map ((principal | user-group)+, backend-principal)>

<!ATTLIST security-map
    name CDATA #REQUIRED>


<!-- principal
    Principal of the Servlet and EJB client

  Used in:
```

```
    security-map
-->
<!ELEMENT principal (#PCDATA)>


<!-- user-group

  Used in:
    security-map
-->
<!ELEMENT user-group (#PCDATA)>


<!-- backend-principal

  Used in:
    security-map
-->
<!ELEMENT backend-principal EMPTY>

<!ATTLIST backend-principal
    user-name CDATA #REQUIRED
    password CDATA #IMPLIED>


<!-- thread-pools

  Used in:
    config
-->
<!ELEMENT thread-pools (thread-pool+)>


<!-- thread-pool

  attributes
    idle-thread-timeout-in-seconds
        idle threads are removed from pool, after this time
    max-thread-pool-size
        Maximum number of threads in the threadpool servicing
        requests in this queue. This is the upper bound on the no. of
```

threads that exist in the threadpool.
min-thread-pool-size
Minimum number of threads in the threadpool servicing requests in this queue. These are created up front when this threadpool is instantiated
num-work-queues
This denotes the total number of work queues that are serviced by this threadpool.
thread-pool-id
This is an id for the work-queue e.g. "thread-pool-1", "thread-pool-2" etc

Used in:
thread-pools
-->
<!ELEMENT thread-pool EMPTY>

<!ATTLIST thread-pool
thread-pool-id CDATA #REQUIRED
min-thread-pool-size CDATA "0"
max-thread-pool-size CDATA "200"
idle-thread-timeout-in-seconds CDATA "120"
num-work-queues CDATA "1">

<!-- property
Syntax for supplying properties as name value pairs

Used in:
admin-object-resource, admin-service, alert-service, appclient-module, audit-module, auth-realm, availability-service, cluster, config, connector-connection-pool, connector-module, connector-resource, custom-resource, das-config, diagnostic-service, domain, ejb-container, ejb-container-availability, ejb-module, ejb-timer-service, event, extension-module, external-jndi-resource, filter-config, group-management-service, http-listener, http-service, iiop-listener, j2ee-application, jacc-provider, java-config, jdbc-connection-pool, jdbc-resource, jms-availability, jms-host, jms-service, jmx-connector, lb-config, lifecycle-module, listener-config, load-balancer, log-service, mail-resource,

```
    manager-properties, mbean, mdb-container, module-log-levels,
    module-monitoring-levels, monitoring-service, node-agent, orb,
    persistence-manager-factory-resource, profiler, provider-config,
    resource-adapter-config, security-service, server,
    session-properties, store-properties, transaction-service,
    virtual-server, web-container, web-container-availability,
    web-module
-->
<!ELEMENT property (description?)>

<!ATTLIST property
    name CDATA #REQUIRED
    value CDATA #REQUIRED>


<!-- system-property
    Syntax for supplying system properties as name value pairs

  Used in:
    cluster, config, domain, server
-->
<!ELEMENT system-property (description?)>

<!ATTLIST system-property
    name CDATA #REQUIRED
    value CDATA #REQUIRED>


<!-- server
    J2EE Application Server Configuration

    Each Application Server instance is a J2EEv1.4 compliant container. One
    server instance is specially designated as the Administration Server in
    SE/EE. User applications cannot be deployed to an Adminsitration Server
    instance.


  children
    application-ref
       References to applications deployed to the server instance
    resource-ref
```

References to resources deployed to the server instance

attributes
config-ref
points to a named config. needed for stand-alone servers. If the server instance is part of a cluster, then it must not be present, and will be ignored.
lb-weight
Each server instance in a cluster has a weight, which may be used to represent the relative processing capacity of that instance. Default weight is 100 for every instance. Weighted load balancing policies will use this weight while load balancing requests within the cluster. It is the responsibility of the administrator to set the relative weights correctly, keeping in mind deployed hardware capacity.
name
name of the server instance.
node-agent-ref
SE/EE only. Specifies the name of the node agent where the server instance is hosted.

Used in:
servers
-->
<!ELEMENT server
(application-ref*, resource-ref*, system-property*, property*)>

<!ATTLIST server
name CDATA #REQUIRED
config-ref CDATA #IMPLIED
node-agent-ref CDATA #IMPLIED
lb-weight CDATA "100">

<!-- application-ref

attributes
disable-timeout-in-minutes
The time, in minutes, that it takes this application to reach a quiescent state after having been disabled

```
    lb-enabled
        A boolean flag that causes any and all load-balancers using
        this application to consider this application unavailable to
        them. Defaults to unavailable (false).

  Used in:
    cluster, server
-->
<!ELEMENT application-ref EMPTY>

<!ATTLIST application-ref
    enabled %boolean; "true"
    virtual-servers CDATA #IMPLIED
    lb-enabled %boolean; "false"
    disable-timeout-in-minutes CDATA "30"
    ref CDATA #REQUIRED>


<!-- resource-ref

  Used in:
    cluster, server
-->
<!ELEMENT resource-ref EMPTY>

<!ATTLIST resource-ref
    enabled %boolean; "true"
    ref CDATA #REQUIRED>


<!-- cluster
    SE/EE Cluster configuration. A cluster defines a homogenous set
    of server instances that share the same applications, resources,
    and configuration.

  children
    server-ref
        list of servers in the cluster

  attributes
    config-ref
```

```
      points to a named config. All server instances in the cluster
      will share this config.
    heartbeat-address
      This is the address (only multicast supported) at which GMS
      will listen for group events.
    heartbeat-enabled
      When "heartbeat-enabled" is set to "true", the GMS services
      will be started as a lifecycle module in each the application
      server in the cluster.When "heartbeat-enabled" is set to
      "false", GMS will not be started and its services will be
      unavailable. Clusters should function albeit with reduced
      functionality.
    heartbeat-port
      This is the communication port GMS uses to listen for group
      events . This should be a valid port number.
    name
      cluster name

  Used in:
    clusters
-->
<!ELEMENT cluster
    (server-ref*, resource-ref*, application-ref*, system-property*,
    property*)>


<!ATTLIST cluster
    name CDATA #REQUIRED
    config-ref CDATA #REQUIRED
    heartbeat-enabled %boolean; "true"
    heartbeat-port CDATA #IMPLIED
    heartbeat-address CDATA #IMPLIED>


<!-- server-ref

  attributes
    disable-timeout-in-minutes
      The time, in minutes, that it takes this server to reach a
      quiescent state after having been disabled
    enabled
```

```
      A boolean flag that causes the server to be enabled to serve
      end-users, or not. Default is to be enabled (true)
    lb-enabled
      A boolean flag that causes any and all load-balancers using
      this server to consider this server unavailable to them.
      Defaults to unavailable (false)
    ref
      A reference to the name of a server defined elsewhere

  Used in:
    cluster, lb-config
-->
<!ELEMENT server-ref (health-checker?)>

<!ATTLIST server-ref
    ref CDATA #REQUIRED
    disable-timeout-in-minutes CDATA "30"
    lb-enabled %boolean; "false"
    enabled %boolean; "true">


<!-- node-agent
    SE/EE Node Controller. The node agent is an agent that manages
    server instances on a host machine.

  attributes
    name
      Node Controller name
    start-servers-in-startup
      If true starts all managed server instances when the Node
      Controller is started.
    system-jmx-connector-name
      The name of the internal jmx connector

  Used in:
    node-agents
-->
<!ELEMENT node-agent (jmx-connector?, auth-realm?, log-service, property*)>

<!ATTLIST node-agent
    name CDATA #REQUIRED
```

```
    system-jmx-connector-name CDATA #IMPLIED
    start-servers-in-startup %boolean; "true">


<!-- lb-config

  attributes
    https-routing
        Boolean flag indicating how load-balancer will route https
        requests. If true then an https request to the load-balancer
        will result in an https request to the server; if false then
        https requests to the load-balancer result in http requests
        to the server. Default is to use http (i.e. value of false);
    monitoring-enabled
        Boolean flag that determines whether monitoring is switched
        on or not. Default is that monitoring is switched off (false)
    name
        Name of the load balancer configuration
    reload-poll-interval-in-seconds
        Maximum period, in seconds, that a change to the load
        balancer configuration file takes before it is detected by
        the load balancer and the file reloaded. A value of 0
        indicates that reloading is disabled. Default period is 1
        minute (60)
    response-timeout-in-seconds
        Period within which a server must return a response or
        otherwise it will be considered unhealthy. Default value is
        60 seconds. Must be greater than or equal to 0. A value of 0
        effectively turns off this check functionality, meaning the
        server will always be considered healthy.
    route-cookie-enabled
        Boolean flag that determines whether a route cookie is or is
        not enabled. Default is enabled (true).

  Used in:
    lb-configs
-->
<!ELEMENT lb-config ((cluster-ref* | server-ref*), property*)>

<!ATTLIST lb-config
    name CDATA #REQUIRED
```

```
    response-timeout-in-seconds CDATA "60"
    https-routing %boolean; "false"
    reload-poll-interval-in-seconds CDATA "60"
    monitoring-enabled %boolean; "false"
    route-cookie-enabled %boolean; "true">


<!-- health-checker
    Each cluster would be configured for a ping based health check
    mechanism.

  attributes
    interval-in-seconds
        Interval, in seconds, between health checks. A value of "0"
        means that the health check is disabled. Default is 30
        seconds. Must be 0 or greater.
    timeout-in-seconds
        Maximum time, in seconds, that a server must respond to a
        health check request to be considered healthy. Default is 10
        seconds. Must be greater than 0.
    url
        URL to ping so as to determine the health state of a
        listener. This must be a relative URL.

  Used in:
    cluster-ref, server-ref
-->
<!ELEMENT health-checker EMPTY>

<!ATTLIST health-checker
    url CDATA "/"
    interval-in-seconds CDATA "30"
    timeout-in-seconds CDATA "10">


<!-- cluster-ref
    Element relating a reference to a cluster to be load balanced to
    an (optional) health-checker

  attributes
    lb-policy
```

load balancing policy to be used for this cluster. Possible values are round-robin , weighted-round-robin or user-defined. round-robin is the default. For weighted-round-robin, the weights of the instance are considered while load balancing. For user-defined, the policy is implemented by a shared library which is loaded by the load balancer and the instance selected is delegated to the loaded module.

lb-policy-module

specifies the absolute path to the shared library implementing the user-defined policy. This should be specified only when the lb-policy is user-defined. The shared library should exist and be readable in the machine where load balancer is running.

ref

A reference to the name of a cluster defined elsewhere

Used in:

lb-config

-->

<!ELEMENT cluster-ref (health-checker?)>

<!ATTLIST cluster-ref
ref CDATA #REQUIRED
lb-policy %lb-policy-type; "round-robin"
lb-policy-module CDATA #IMPLIED>

<!-- message-security-config

The message-security-config element defines the message layer specific provider configurations of the application server.

All of the providers within a message-security-config element must be able to perform authentication processing at the message layer defined by the value of the auth-layer attribute.

attributes

default-client-provider

used to identify the client provider to be invoked for any application for which a specific client provider has not been

bound.
default-provider
used to identify the server provider to be invoked for any application for which a specific server provider has not been bound.

When a default provider of a type is not defined for a message layer, the container will only invoke a provider of the type (at the layer) for those applications for which a specific provider has been bound.

Used in:
security-service
-->
<!ELEMENT message-security-config (provider-config+)>

<!ATTLIST message-security-config
auth-layer %message-layer; #REQUIRED
default-provider CDATA #IMPLIED
default-client-provider CDATA #IMPLIED>

<!-- provider-config
The provider-config element defines the configuration of an authentication provider.

A provider-config with no contained request-policy or response-policy sub-elements, is a null provider. The container will not instantiate or invoke the methods of a null provider, and as such the implementation class of a null provider need not exist.

children
request-policy
defines the authentication policy requirements associated with the request processing performed by the authentication provider.
response-policy
defines the authentication policy requirements associated with the response processing performed by the authentication provider.

```
  attributes
    class-name
       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.
    provider-id
       Identifier used to uniquely identify this

       provider-config
       element
    provider-type
       defines whether the provider is a client authentication
       provider or a server authentication provider.

  Used in:
    message-security-config
-->
<!ELEMENT provider-config (request-policy?, response-policy?, property*)>

<!ATTLIST provider-config
    provider-id CDATA #REQUIRED
    provider-type (client | server | client-server) #REQUIRED
    class-name CDATA #REQUIRED>


<!-- request-policy
    Used to define the authentication policy requirements associated
    with the request processing performed by an authentication
    provider (i.e. when a client provider's

    ClientAuthModule.initiateRequest()
    method is called or when a server provider's
```

```
    ServerAuthModule.validateRequest()
    method is called).

  attributes
    auth-recipient
       defines a requirement for message layer authentication of the
       reciever of a message to its sender (e.g. by XML encryption).
       before-content
          indicates that recipient authentication (e.g. encryption)
          is to occur before any content authentication (e.g.
          encrypt then sign) with respect to the target of the
          containing auth-policy.
       after-content
          indicates that recipient authentication (e.g. encryption)
          is to occur after any content authentication (e.g. sign
          then encrypt) with respect to the target of the
          containing auth-policy.
    auth-source
       defines a requirement for message layer sender authentication
       (e.g. username password) or content authentication (e.g.
       digital signature).

  Used in:
    provider-config
-->
<!ELEMENT request-policy EMPTY>

<!ATTLIST request-policy
    auth-source (sender | content) #IMPLIED
    auth-recipient (before-content | after-content) #IMPLIED>



<!-- response-policy
    Used to define the authentication policy requirements associated
    with the response processing performed by an authentication
    provider (i.e. when a client provider's

    ClientAuthModule.validateResponse()
    method is called or when a server provider's

    ServerAuthModule.secureResponse()
```

```
    method is called).

  attributes
    auth-recipient
        defines a requirement for message layer authentication of the
        reciever of a message to its sender (e.g. by XML encryption).
        before-content
            indicates that recipient authentication (e.g. encryption)
            is to occur before any content authentication (e.g.
            encrypt then sign) with respect to the target of the
            containing auth-policy.
        after-content
            indicates that recipient authentication (e.g. encryption)
            is to occur after any content authentication (e.g. sign
            then encrypt) with respect to the target of the
            containing auth-policy.
    auth-source
        defines a requirement for message layer sender authentication
        (e.g. username password) or content authentication (e.g.
        digital signature).

  Used in:
    provider-config
-->
<!ELEMENT response-policy EMPTY>

<!ATTLIST response-policy
    auth-source (sender | content) #IMPLIED
    auth-recipient (before-content | after-content) #IMPLIED>



<!-- web-service-endpoint
    This specifies configuration for a web service end point. This
    web service end point could be JAXRPC or JSR-109 web service. It
    contains configuration about Monitoring, Transformation rules and
    Monitoring Log.

  attributes
    jbi-enabled
        when false, it disables the visibility of this endoint as a
        service in JBI
```

```
    max-history-size
        maximum number of monitoring records stored in history for
        this end point
    monitoring
        monitoring level for this web service.
    name
        fully qualified web service name. Format:
        |ModuleName|#|EndpointName|, if the web service endpoint
        belongs to an application. (Parent of this element is
        j2ee-application). |EndpointName|, if the web service
        endpoint belongs to stand alone ejb-module or web-module.
        (Parent of this element is either ejb-module or web-module).

  Used in:
    ejb-module, j2ee-application, web-module
-->
<!ELEMENT web-service-endpoint (registry-location*, transformation-rule*)>

<!ATTLIST web-service-endpoint
    name CDATA #REQUIRED
    monitoring %monitoring-level; "OFF"
    max-history-size CDATA "25"
    jbi-enabled %boolean; "true">


<!-- registry-location
    Specifies the registry where web service end point artifacts are
    published.

  Used in:
    web-service-endpoint
-->
<!ELEMENT registry-location EMPTY>

<!ATTLIST registry-location
    connector-resource-jndi-name CDATA #REQUIRED>


<!-- transformation-rule
    Specifies configuration for a XSLT transformation rule.
```

```
  attributes
    apply-to
       - "request": transformations are applied to request in the order in
       which they are specified.

       - "response": transformation is applied to response in the order in
       which they are specified.

       - "both": transformation rule is applied to request and response. The
       order is reversed for response.

    enabled
       if false, this transformation rule is disabled.
    name
       name of the transformation rule
    rule-file-location
       location of rule file to do the transformation. Only XSLT
       files are allowed. Default location is:
       ${com.sun.aas.instanceRoot}/generated/xml/*appOrModule*/*xslt-
       ilename*/ Absolute paths can also be specified.

  Used in:
    web-service-endpoint
-->
<!ELEMENT transformation-rule EMPTY>

<!ATTLIST transformation-rule
    name CDATA #REQUIRED
    enabled %boolean; "true"
    apply-to %apply-to-type; "request"
    rule-file-location CDATA #REQUIRED>


<!-- load-balancers

  Used in:
    domain
-->
<!ELEMENT load-balancers (load-balancer*)>
```

```
<!-- load-balancer
    known properties:

    device-host - Host name or IP address for the device

    device-admin-port - Device administration port number

    ssl-proxy-host - proxy host used for outbound HTTP

    ssl-proxy-port - proxy port used for outbound HTTP


  attributes
    auto-apply-enabled
        when true, immediately push changes to lb config to the
        physical load balancer
    lb-config-name
        name of the lb-config used by this load balancer
    name
        name of the load balancer

  Used in:
    load-balancers
-->
<!ELEMENT load-balancer (property*)>

<!ATTLIST load-balancer
    name CDATA #REQUIRED
    lb-config-name CDATA #REQUIRED
    auto-apply-enabled %boolean; "false">


<!-- mbean

  attributes
    enabled
    impl-class-name
        A String that represents fully qualified class name of MBean
        implementation. This is read-only.
    name
        A String that represents the name of the MBean. It is
```

required that the name is valid to represent a "value" of a property in the property-list of an MBean ObjectName. The name must be specified and is a primary key for an MBean. An invalid name implies failure of operation.

object-name

A String that represents a system-generated Object Name for this MBean.

object-type

A String representing whether it is a user-defined MBean or a System MBean.

Used in:

applications

-->

<!ELEMENT mbean (description?, property*)>

<!ATTLIST mbean
name CDATA #REQUIRED
object-type %object-type; "user"
impl-class-name CDATA #REQUIRED
object-name CDATA #IMPLIED
enabled %boolean; "true">

<!-- extension-module

attributes

availability-enabled

The exact semantics of availability being enabled for an extension module are undefined at this time. If this attribute is missing, it defaults to "false".

directory-deployed

This attribute indicates whether the application has been deployed to a directory or not

libraries

System dependent path separator [: for Unix/Solaris/Linux and ; for Windows] separated list of jar paths. These paths could be either relative [relative to {com.sun.aas.instanceRoot}/lib/applibs] or absolute paths. These dependencies appears *after* the libraries defined in classpath-prefix in the java-config and *before* the

application server provided over-rideable jar set. The
libraries would be made available to the application in the
order in which they were specified.
module-type
String representing the module type. This module type will be
used by the runtime to find the appropriate extension
container.

Used in:
applications
-->
<!ELEMENT extension-module (description?, property*)>

<!ATTLIST extension-module
name CDATA #REQUIRED
location CDATA #REQUIRED
module-type CDATA #REQUIRED
object-type %object-type; "user"
enabled %boolean; "true"
libraries CDATA #IMPLIED
availability-enabled %boolean; "false"
directory-deployed %boolean; "false">

<!-- jms-availability

attributes
availability-enabled
This boolean flag controls whether the MQ cluster associated
with the application server cluster is HA enabled or not. If
this attribute is "false", then the MQ cluster pointed to by
the jms-service element is considered non-HA. JMS Messages
are not persisted to a highly available store. If this
attribute is "true" the MQ cluster pointed to by the
jms-service element is a HA cluster and the MQ cluster uses
the database pointed to by mq-store-pool-name to save
persistent JMS messages and other broker cluster
configuration information. Individual applications will not
be able to control or override MQ cluster availability
levels. They inherit the availability attribute defined in
this element. If this attribute is missing, availability is

```
        turned off by default [i.e. the MQ cluster associated with
        the AS cluster would behave as a non-HA cluster]
    mq-store-pool-name
        This is the jndi-name for the JDBC Connection Pool used by
        the MQ broker cluster for use in saving persistent JMS
        messages and other broker cluster configuration information.
        It will default to value of store-pool-name under
        availability-service (ultimately "jdbc/hastore").

  Used in:
    availability-service
-->
<!ELEMENT jms-availability (property*)>

<!ATTLIST jms-availability
    availability-enabled %boolean; "false"
    mq-store-pool-name CDATA #IMPLIED>


<!-- management-rules
    Container for self management rules

  attributes
    enabled
        Acts as high level switch for disabling all the defined
        rules. If set to "false" all the configured rules would
        disabled. If set to "true", enabled state of a particular
        rule will be decided at that rule level.

  Used in:
    config
-->
<!ELEMENT management-rules (management-rule*)>

<!ATTLIST management-rules
    enabled %boolean; "true">


<!-- management-rule
    Defines the configured self management rule
```

```
  attributes
    enabled
       Determines whether the rule is enabled or not. Default value
       is false.
    name
       Name of the management rule

  Used in:
    management-rules
-->
<!ELEMENT management-rule (event, action?, description?)>

<!ATTLIST management-rule
    name CDATA #REQUIRED
    enabled %boolean; "true">



<!-- event
    Defines the event associated with the configured rule. For each
    configured rule there exists one event associated with it.

  attributes
    level
       Specifies at what level to record the event occurance in
       server log file. Default value is INFO
    record-event
       Specifies whether the occurance of the event is to be logged
       or not. By default this would be true. If no action is
       specified, the event would be recorded.
    type
       Identifies the configured event as one of the predefined
       event types.

  Used in:
    management-rule
-->
<!ELEMENT event (description?, property*)>

<!ATTLIST event
    type %event-type; #REQUIRED
    record-event %boolean; "true"
```

```
    level %log-level; "INFO">


<!-- action
    Defines the action MBean associated with the event.

  attributes
    action-mbean-name
        identifies the name of the action MBean.

  Used in:
    management-rule
-->
<!ELEMENT action EMPTY>

<!ATTLIST action
    action-mbean-name CDATA #REQUIRED>
```