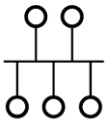

Orbix®

Release Notes

Version 6.2, June 2005

Making Software Work Together™

Updated: 08-Jan-2007

Contents

Orbix 6.2 Service Pack 1 Release Notes

In this document

This document contains the following sections:

Platforms and Features Removed

The following platforms have been removed in the Orbix 6.2 release:

- Red Hat Linux 7.2 is replaced by Red Hat Enterprise Linux AS 3.0.
- Gcc 3.2.2 on Linux is replaced by Gcc 3.3.3.
- Windows NT has been replaced by Windows 2003.

The following features have been removed in the Orbix 6.2 release:

- Orbix Web services development tools.
- Orbix .NET Connector.
- IONA Medic.

IONA provides support for enterprise middleware integration, Web services integration, J2EE integration and .NET integration through its Artix product range. Contact your IONA account manager or sales representative for more information.

CORBA Compliance

Orbix 6.2 complies with the following specifications:

- CORBA 2.6.
- GIOP 1.2 (default), 1.1, and 1.0.
- C++ Language Mapping (formal/99-07-41).
- IDL-to-Java Language Mapping (formal/99-07-53).
- Object transaction service (OTS) 1.1 and 1.2.

LDAP Support

The IONA security platform integrates with the Lightweight Directory Access Protocol (LDAP) enterprise security infrastructure by using an LDAP adapter. You can use the Orbix security service's LDAP adapter with any LDAP v.3 compatible system. If you are using LDAP v.2, we recommend that you write a custom adapter.

For more information on Orbix' LDAP support, see the Orbix Security Guide.

New Features in Orbix 6.2

Orbix 6.2 includes the following new features:

- "Supported Platforms and Compilers".
- "High Availability".
- "Security".
- "Management"
- "Extensible Configuration".
- "Compression Plug-in".
- "Buffered Logging".

Supported Platforms and Compilers

Orbix 6.2 includes support for the following new platforms and compilers:

- AIX 5.2 and Visual Age 6.0.
- Windows 2003, Visual C++ 6.0 and Visual Studio .NET 2003 7.1.
- Full enterprise support for Red Hat Linux Advanced Server (AS) 3.0.
- 64-bit JVM support on Sun Solaris 9.
- JDK 1.4.2.
- Sun Studio 8.
- HP-UX 11i on Itanium.

See the *Installation Prerequisites* section in the Orbix 6.2 Installation Guide for full details of all supported platforms and compilers.

High Availability

Orbix 6.2 includes the following new high availability features:

- Berkeley DB replication.
- Performance enhancements.
- Slaves dynamically promoted to master.

Berkeley DB replication

In Orbix 6.2, changes have been made at the Berkeley DB level. Berkeley DB has the ability to propagate replication data between different instances of the database. Orbix inherits this ability to replicate, and propagates the data across the network through the persistent state service (PSS) layer. This provides a dramatic performance improvement when slaves are being promoted to master. Unlike in previous releases of Orbix, the database does not need to be opened, closed and recovered with each replication update at a slave replica.

Slaves dynamically promoted to master

If the master fails, a slave is automatically promoted without the need to restart any services or make any configuration changes. During the promotion period, write operations are blocked until a new master is chosen or until a configurable timeout occurs. Berkeley DB has an election protocol that guarantees that the most appropriate slave is promoted when the master fails. The most up-to-date slave is always elected first. If all slaves are at the same level, then they are promoted according to a priority setting. If no priorities are assigned, slaves are promoted randomly.

A slave replica can only be promoted to a master if there are a majority of slave replicas running. As a consequence, a minimum of three replicas—one master and two slaves—is required to support slave promotion. It is possible, however, to workaround this. A slave can be dynamically promoted to master when the master fails in a replica group of exactly two replicas (one master and one slave), by setting the configuration variable `plugins:pss_db:envs:<env-name>:allow_minority_master` to `"true"`. Note, this only applies in cases where there are exactly two replicas—one master and one slave—in a replica group.

Another change from previous Orbix releases is that all replicas start up as slaves. They call an election to decide which replica is to be the master. In order for the election to proceed, a majority of replicas must be running; for example, in a replica group of three, at least two replicas must be running, but in a replica group of six, at least four replicas must be running before an election can take place. Write operations are blocked until a master is chosen.

More information

For more detail on the high availability features in Orbix 6.2, see the Orbix Administrator's Guide and the Orbix CORBA Programmer's Guides.

Security

Orbix 6.2 includes the following new security features:

- "Clustered security service"
- "Centralized ACL policy definition"
- "Replaceable ACL engine"
- "Automatic warnings on SSL certificates"
- "Support for external bridging to a CSIv2 or Orbix security domain from a non-CORBA technology domain.".

Clustered security service

Multiple security servers can be deployed to remove any single points of failure through automatic failover to backup servers (over IIOP/TLS secured connections). Orbix security supports load balancing across security server instances in a security service cluster.

In addition, security servers can be federated so that you only need to sign on once to have access to multiple security domains.

Centralized ACL policy definition

Orbix 6.2 introduces a new option for centralized access control list (ACL) policy definition. By default, a secure Orbix application is configured to store its ACL locally. In large deployments, therefore, ACL files might be scattered over many hosts. From an administration point of view, however, it is often more convenient to gather ACL files onto a central host. Orbix 6.2 enables you to do just that. You can configure your secure applications to use a centralized ACL repository. As a result, you can administer all of the ACL data in one place, making it easier to update and maintain.

Replaceable ACL engine

The authorization engine can be replaced with a custom ACL implementation or with a third-party ACL engine such as Netegrity or Oblix. This custom ACL implementation can access IONA Security Service authentication information to make its access decisions. Support for replacing the ACL engine is available in for both local and centralized ACL modes.

Automatic warnings on SSL certificates

Orbix 6.2 issues automatic warnings when SSL certificates near their expiration date or meet some other user-specified criteria.

WARNING: Demonstration certificates should never be used in a production system. They are only intended for demonstration, development and testing purposes. The security of your system depends on these certificates being replaced with a securely generated set of certificates.

Support for external bridging to a CSIv2 or Orbix security domain from a non-CORBA technology domain.

The key requirement for secure bridging from a non-CORBA technology domain is the ability to propagate security credentials into the CORBA domain. Two new IDL interfaces, `IT_CSI::CSICurrent2` and `IT_CSI::CSICurrent3`, support this capability. For details, see the following reference guide pages:

http://www.iona.com/support/docs/orbix/6.2/reference/corba_pref/cpp/IT_CSI/CSICurrent2.html

http://www.iona.com/support/docs/orbix/6.2/reference/corba_pref/cpp/IT_CSI/CSICurrent3.html

More information

For more information on the Orbix 6.2 security features, see the Orbix Security Guide.

Management

Orbix 6.2 includes the following new management features:

- Integration with HP OpenView Enterprise Management System.
- Client-side performance logging, which gives metrics on server availability and response time.
- Managed entity (`MBean`) monitoring plug-in that gathers statistics for the log file on whatever is instrumented.
- Orbix work queue instrumented and available in as a managed entity (`MBean`).
- New `itadmin` logging commands.
- New `itadmin` notification channel commands.

Integration with HP OpenView

Hewlett-Packard has produced a smart plug-in for integrating Orbix with the HP OpenView Enterprise Management System (EMS). This enables you to monitor Orbix-based applications using HP OpenView tools, and perform tasks such as starting and stopping servers.

For more information, see the following HP links:

- Smart Plug-in for IONA Orbix
- Smart Plug-in for IONA Orbix Administrator's and User's Guide

Performance logging

Orbix 6.2 introduces client-side performance logging. This gives metrics on server availability and response time. It does not require any changes to code. A simple configuration setting is all that is required to set this in action.

For more information, see the Orbix Management User's Guide.

MBean monitoring plug-in

Orbix 6.2 also includes a plug-in that monitors managed entities (`MBean`s). It gathers statistics on whatever has been instrumented and stores them in the log file. For example, the Orbix work queue has been instrumented and its length can be monitored. In addition, any application-level managed entities can be monitored.

For more information, see the Orbix Management User's Guide and the Orbix Management Programmer's Guide.

itadmin logging commands

Lastly, Orbix 6.2 includes new `itadmin` commands enable the event log filters to be updated dynamically from the `itadmin` command line. They are:

`itadmin logging get -orbname` *<orb name>*
`itadmin logging set -orbname` *<orb_name>* `-value` *<new event log filter>*

For more information, see the Orbix Administrator's Guide.

itadmin notification channel commands

Orbix 6.2 includes new `itadmin` notification channel commands that enable the creation and modification of notification channel quality of service (QOS) properties.

For more information, see the `itadmin nc qos` command in the Orbix Administrator's Guide.

Extensible Configuration

Orbix 6.2 supports extensible configuration. Everything does not have to be configured up front when a system is first deployed. Domain functionality can be extended at a later stage by deploying, for example, a naming service, or by adding or deleting service replicas.

For more information, see the Orbix Deployment Guide.

Compression Plug-in

Orbix 6.2 includes a ZIOP compression plug-in that provides optional compression of GIOP messages on the wire. Compressed and uncompressed transports can be mixed. This can provide significant performance improvements on low bandwidth networks. The performance improvements depend on the network as well as the message data. If, for example, the requests contain JPEG images, there will be virtually no compression, whereas with repetitive string data, there will be good compression.

For more information, see the Orbix Administrator's Guide and the Orbix CORBA Programmer's Guide for more detail.

Buffered Logging

Orbix 6.2 supports buffered logging of the output stream. The logs are buffered and output to file when the buffer reaches a certain size and an adequate period of time has lapsed. Both of these values are configurable. Buffered logging improves the performance of servers that log extensively.

For more information, see the Orbix Administrator's Guide.

New Features in Orbix 6.2 Service Pack 1

Orbix 6.2 Service Pack 1 includes the following new features:

- "Supported Platforms and Compilers"
- "Per-Client Activation".
- "Addressing Services with Corbaloc URLs".
- "New Security Policies"
- "SSL/TLS Mechanism Policy Can Specify Multiple Protocols"

Supported Platforms and Compilers

Orbix 6.2 Service Pack 1 includes support for the following new platforms:

- Solaris 10 on SPARC
- 64-bit support on RedHat Linux AS 3.0. (Both 32- and 64-bit are installed so the installation size has increased as a result)

See the *Installation Prerequisites* section in the Orbix 6.2 Installation Guide for full details of all supported platforms and compilers.

Per-Client Activation

Service Pack 1 includes support for *per-client* activation of server processes. This provides similar functionality to the Orbix 3 *per-client-pid* activation mode. Per-client activation is similar to on-demand activation, but maintains a one-to-one mapping between clients and server processes. This ensures that a server process is never shared between multiple clients.

To register a process for per-client activation use the `itadmin process create` command, and specify `per_client` for the startup-mode. For example:

```
itadmin process create
 -node_daemon iona_services.node_daemon.oregon
 -pathname "/usr/app/myapp "
 -startupmode per_client
 -args "--home /usr/app -ORBname %o" my_app
```

For more information, see Chapter 4 of the Orbix Administrator's Guide.

Addressing Services with Corbaloc URLs

Service Pack 1 includes support for addressing services using corbaloc URLs. All Orbix services that had not already done so in previous releases now use a collocated plain text key forwarder. This enables them to register named keys for object references published when the service runs in prepare mode. The services register named keys regardless of their persistence mode. For debugging purposes, even indirect persistent services can be addressed using a corbaloc URL (provided that the port information is available).

Services that have not previously registered such named keys, or have done so only if the service was configured as direct persistent, revert to their original behaviour when you set a configuration variable for that service to `true`. These variables take the format: `plugins:`*`service_name`*`:advertise services`. For example: `plugins:naming:advertise_services`. For more details, see the Orbix Configuration Reference.

In this release, the following key strings were registered with the collocated plain text key forwarder, in this order:

1. Existing, previously used, but undocumented key strings in the collocated plain text forwarder (for example, JMS).
2. Key string used in the implementation repository (IMR), if the reference was registered in the IMR's plain text key registry (for example, IFR).
3. Initial reference name used in Orbix configuration (`initial_references:`*`ReferenceName`*`:reference`), as generated by the Orbix configuration tools (for example, Transaction monitor).
4. Prefix of the published IOR (obtained when service is run in prepare mode).

The key strings used in the collocated plain text key forwarder may differ from those used in the IMR. These are created as before, and the same service may be addressed using corbaloc URLs with different object addresses. For a full listing of the key strings, initial references and IOR prefixes for Orbix services, see Appendix E of the Orbix Administrator's Guide.

New Security Policies

The IT_CSI AuthenticationServicePolicy and AttributeServicePolicy policies (and the associated structs) are still supported but are deprecated. Customers should be able to use the following new policies. (Refer to the Security Documentation for more details).

```
struct AttributeServiceProtocolClient
{
    CSIIOP::AssociationOptions auth_over_trans_supports;
    CSIIOP::AssociationOptions attribute_service_layer_supports;
};

struct AttributeServiceProtocolServer
{
    string server_domain_name;
    CSIIOP::AssociationOptions auth_over_trans_supports;
    CSIIOP::AssociationOptions auth_over_trans_requires;
    CSIIOP::AssociationOptions attribute_service_layer_supports;
};

local interface AttributeServiceProtocolClientPolicy : CORBA::Policy
{
    readonly attribute AttributeServiceProtocolClient
   attribute_service_protocol_client;
};

local interface AttributeServiceProtocolServerPolicy : CORBA::Policy
{
    readonly attribute AttributeServiceProtocolServer
   attribute_service_protocol_server;
};
```

By default the old legacy polices will be used but you can switch to the new policies by setting the following variable to true

```
plugins:csi:use_legacy_policies = "false";
```

SSL/TLS Mechanism Policy Can Specify Multiple Protocols

The `policies:iiop_tls:mechanism_policy:protocol_version` configuration variable has been modified so that it now accepts a list of protocols, instead of just a single protocol value. For example:

```
# Orbix Configuration File
policies:iiop_tls:mechanism_policy:protocol_version = ["TLS_V1",
   "SSL_V3"];
```

During the SSL/TLS handshake, the highest common protocol will be negotiated.

If you have an Orbix server that communicates with a CORBA client running on a mainframe platform, you should note that the special protocol value `SSL_V2V3` is no longer supported. Instead, for this Orbix server, you should configure it to accept SSLv2 hellos by setting the following configuration variable to `true`:

```
# Orbix Configuration File
policies:iiop_tls:mechanism_policy:accept_v2_hellos = "true";
```

Known Issues

The following known issues exist in Orbix 6.2:

Installation and Configuration

- Installing Orbix Visual Studio wizards.
- Uppercase and mixed case hostnames.
- Using the -background flag on Windows.
- Tru64 UNIX and JDK 1.4.2.
- IRIX and JDK 1.4.1
- Allocating buffers using Java NIO.
- Running itconfigure on UNIX with JDK 1.4.x

General

- Multicast consumers
- CSI Service Context Error Message
- Files specifying incorrect location for omg.jar
- Compiling on AIX
- Windows XP Service Pack 2 and PowerBuilder 7.0

Security

- Launching CORBA consoles with security enabled.
- Secure/semi-secure applications on JDK 1.4.2.
- Delayed credentials gathering with the SChannel toolkit and COMet.
- Interoperability with Orbix 3.3.6 or lower.

Management

- Running web console with HP-UX JDK 1.4.2

Installation and Configuration

The installation and configuration issues are as follows:

Installing Orbix Visual Studio wizards

In some cases, the Orbix Visual Studio wizards will not be installed automatically by the installer. See the *Orbix Installation Guide* for instructions on how to manually install these wizards.

Uppercase and mixed case hostnames

Specify lowercase hostnames when configuring Orbix. Using uppercase hostnames, or a mix of lowercase and uppercase hostnames may result in problems.

Using the -background flag on Windows

On Windows, it is not possible to run a service with the `-background` flag if the `principal_sponsor:csi:auth_method_data` is not specified in configuration. If the service must run in the background, it is recommended that a password file is used, and that access to that password file is restricted to `Administrator` only. For example:

```
principal_sponsor:csi:auth_method_data = ["username=Administrator",
"password_file=U:\secure_directory\secret.pwf", "domain=IONA"];
```

Tru64 UNIX and JDK 1.4.2

When deploying on Tru64 (OSF1) using JDK 1.4.2, you require 256 MB of minimum memory. This extra memory is not required for previous JDK versions, or for other operating systems.

If you want to use a domain created previously using Orbix 6.1 and JDK 1.4.1 (or lower), and run the services with JDK 1.4.2, you must edit the configuration and change the following variable for all Java-based services.

```
plugins:java_server:X_options = ["rs"];
```

should now be

```
plugins:java_server:X_options = ["rs", "ms128M", "mx256M"];
```

IRIX and JDK 1.4.1

The `jdk 1.4.1_x` implemented by SGI for IRIX does not include support for the java endorsed standards mechanism. You must use the `-Xbootclasspath` java command-line argument to ensure that the JDK uses IONA's implementation of the OMG classes rather than those in the JDK; for example:

```
-Xbootclasspath/p:$IT_PRODUCT_DIR/lib/art/omg/1.2/omg.jar
```

Allocating buffers using Java NIO

The Java New Input/Output (NIO) transport can be configured to allocate buffers that are either backed by Java heap memory or native memory. Because of a limitation in the Java VM, heap buffers currently scale better on multi-processor machines, while native buffers perform better on single CPU machines. If heap buffers are to be used instead of native buffers (the default), set `plugins:atli2_ip:nio:allocate_heap_byte_buffer` to `true`.

Running itconfigure on UNIX with JDK 1.4.x

When run under JDK 1.4.x, `itconfigure` stores location details of the five most recently created/opened domains as user preferences. This might fail on UNIX platforms if `.java/.userPrefs` cannot be created under `/tmp`, or if it exists but is not writable. To workaround this issue, comment out line 223 in `$IT_PRODUCT_DIR/asp/6.2/bin/itconfigure`:

```
#jdk_user_preferences_root=-Djava.util.prefs.userRoot=/tmp
```

This will result in `itconfigure` using the default value, which is `System.getProperty("user.home")`.

General

General issues are as follows:

Multicast consumers

Multicast consumers are not supported on Irix. If this feature is required, please contact IONA Support.

CSI Service Context Error Message

When preparing a Naming or Locator Service Slave in Windows 2000, the following message may be logged by the Locator Service Master:

```
(IT_CSI:6) E - Bad or no CSI service context received in reply.
```

This message can be safely ignored.

Files specifying incorrect location for omg.jar

A number of files specify an incorrect location for the `omg.jar` file. The incorrect location being used is:

```
$IT_PRODUCT_DIR/lib/art/omg/5/omg.jar
```

The correct location is:

```
$IT_PRODUCT_DIR/lib/art/omg/1.2/omg.jar
```

The files using the incorrect location include the Java demo readme files and the following files which are in the `<install-dir>asp/6.2/bin` directory:

```
it_java.tcl, itconfigexplorer, itconfigure, itdeployer,
itiadmin_command, itlogging_console, itnotify, itnotify_console,
ittrader_console.
```

Compiling on AIX

When linking C++ applications, Visual Age versions 5 and 6 generate duplicate symbol warnings for functions that exist in multiple object files. You can safely ignore these warnings. They are generated because the IBM C++ compiler, in accordance with *ISO/IEC 14882:1998(E): Programming Languages: C++ (see section 3.5, Program and Linkage)*, give non-inline functions eternal linkages.

If you do not want to receive these warnings, you can pass the compiler the `-qstaticinline` flag. This will generate internal linkages for non-inline functions. Alternatively, you can specify the `-bhalt:5` flag when linking. This also suppresses the warning messages.

Windows XP Service Pack 2 and PowerBuilder 7.0

When running on Windows XP with Service Pack 2 applied, clients developed using PowerBuilder 7.0 cannot be used to communicate with a CORBA server using COMet.

Security

The security issues are as follows:

Launching CORBA consoles with security enabled

If you create a domain with security enabled, whether it is a secure or semi-secure domain, and you want to launch the following CORBA consoles:

```
ittrader_console
itnotify_console
itlogging_console
```

You must either:

- Modify the console launch script; or

- Add the '-ORBname' parameter to the command line

Modify the console launch script

You must modify the following console launch scripts if you want to launch the consoles from the itconfigure GUI:

```
<install_dir>/asp/6.2/bin/itnotify_console.bat/.sh
<install_dir>/asp/6.2/bin/itlogging_console.bat/.sh
<install_dir>/asp/6.2/bin/ittrader_console.bat/.sh
```

For example, the following shows a modified itnotify_console.bat script. Find the relevant code in the script and append it with '-ORBname iona_utilities.admin' as demonstrated below:

```
if %it_start_in_bg%==0 "%JAVA_HOME%\bin\java" %java_flags%
-Djava.endorsed.dirs="%it_my_product_dir%\lib\art\omg\5"
-Dorg.omg.CORBA.ORBClass=com.iona.corba.art.artimpl.ORBImpl
-Dorg.omg.CORBA.ORBSingletonClass=com.iona.corba.art.artimpl.ORBSing
   leton
-classpath "%it_my_classpath%"  com.iona.corba.notify.console.Main
%it_param_list% -ORBname iona_utilities.admin

if %it_start_in_bg%==1 start "" "%JAVA_HOME%\bin\javaw" %java_flags%
-Djava.endorsed.dirs="%it_my_product_dir%\lib\art\omg\5"
-Dorg.omg.CORBA.ORBClass=com.iona.corba.art.artimpl.ORBImpl
-Dorg.omg.CORBA.ORBSingletonClass=com.iona.corba.art.artimpl.ORBSing
   leton
-classpath "%it_my_classpath%"  com.iona.corba.notify.console.Main
%it_param_list% -ORBname iona_utilities.admin
```

The same modifications must be made to the logging console and the trader console launch scripts.

Add the '-ORBname' parameter to the command line

If you want to launch the consoles from the command line, and have not modified the console launch scripts, you must pass in the following parameter:

```
-ORBname iona_utilities.admin
```

For example:

```
itnotify_console -ORBname iona_utilities.admin
```

Secure/semi-secure applications on JDK 1.4.2

Using JDK 1.4.2, you must have unlimited cryptography (JCE) policy files installed in your JRE. If you do not, you may encounter the following error when running secure/semi secure applications:

```
"Limited strength policy files are installed in this JVM(1.4):
"$JAVA_HOME". By default, Orbix TLS works with the limited JDK policy
but to use extra strength cryptography such as DES ciphersuites or
large key sizes, then you must install the unlimited cryptography
(JCE) policy files available at
http://java.sun.com/products/jce/index-14.html#UnlimitedDownload";
```

Downloading and installing the unlimited policy JARs from the location referenced in the error message will correct these issues.

Delayed credentials gathering with the SChannel toolkit and COMet

If you are using SChannel and OrbixCOMet, and you have configured delayed credential gathering, your application may appear to hang.

This is because the SChannel plug-in will prompt with a list of available credentials. This prompting is sent to standard out, which OrbixCOMet does not display.

The workaround is to either turn off delayed credentials gathering, or implement your own credentials prompt interface. For more details, and a copy of the IDL interface, please contact IONA Support.

Interoperability with Orbix 3.3.6 or lower

The TLS handshake protocol version has changed in Orbix 6.2 Service Pack 1. By default, Orbix clients now send a TLSv1 hello instead of an SSLv3 hello. This causes handshake failures when interoperating with Orbix 3.3.6 or lower, because these earlier Orbix products do not understand TLSv1.

To work around this problem, you can make the Orbix 6.2.1 client use SSLv3 by setting the client's mechanism policy as follows:

```
# Orbix Configuration File
policies:iiop_tls:mechanism_policy:protocol_version = "SSL_V3";
```

This configuration setting forces Orbix 6.2.1 to use the SSLv3 protocol.

For more details about the changes that have been made to the mechanism policy in Orbix 6.2.1, see "SSL/TLS Mechanism Policy Can Specify Multiple Protocols" on page 11.

Management

The management issues are as follows:

Running web console with HP-UX JDK 1.4.2

There is a bug in the HP-UX JDK 1.4.2 `javac` API, in all versions prior to 1.4.2_05. The `javac` API does not accept certain compiler arguments. This may affect you when running the IONA Administrator Web Console. If you do encounter this issue you will see the following type of error message:

```
org.apache.jasper.JasperException: Unable to compile class for
   JSPUsage:
jsp-&gt;javac &lt;options&gt; &lt;source files&gt;
where &lt;options&gt; includes:
-g Generate all debugging info
-g:none Generate no debugging info
-g:{lines,vars,source} Generate only some debugging info
-O Optimize; may hinder debugging or enlarge class files
-nowarn Generate no warnings
-verbose Output messages about what the compiler is doing
-deprecation Output source locations where deprecated APIs are used
-classpath &lt;path&gt; Specify where to find user class files
-sourcepath &lt;path&gt; Specify where to find input source files
-bootclasspath &lt;path&gt; Override location of bootstrap class
   files
-extdirs &lt;dirs&gt; Override location of installed extensions
-d &lt;directory&gt; Specify where to place generated class files
-encoding &lt;encoding&gt; Specify character encoding used by source
   files
-target &lt;release&gt; Generate class files for specific VM version
   at
org.apache.jasper.compiler.Compiler.compile(Compiler.java:285
at
org.apache.jasper.servlet.JspServlet.loadJSP(JspServlet.java:548)
```

Installing the latest JDK (1.4.2_06) from the HP website (http://www.hp.com/products1/unix/java/versions/) should resolve this problem.

Bugs Fixed in Orbix 6.2

The following bugs have been fixed in Orbix 6.2:

Bug	Description
69488	`TypeId` string returned by the CORBA call `ids()` non-compliant.

Bug	Description
69454	`idl -jbase=-ETRUE` should also initialize bounded strings with empty strings.
69390	`IT_LOC_ActivePOARegistryImpl::find()` does not check if a returned reference to a POA is `_nil()`
69379	Uncaught `IT_TSRuntime` exception in `IT_OTS_Lite_TimeoutManager::run()`
69307	Node daemon reports process as active after it has exited. A new `itadmin` command, `itadmin process kill -force <process_name>`, forces cleanup of persistent information held in the node daemon for a previously active process. See the *Orbix Administrator's Guide* for more detail.
69290	Direct persistence and replica failover broken in Orbix 6.1 Service Pack 1 Java (SSL only).
69279	Selecting "Fully Qualified Hostname" in itconfigure's **Expert** panel does not work.
69276	`CORBA::Context` ignored if `ignore_message_not_consumed` set to `true`.
69272	`BAD_PARAM` exception thrown when bidirectional GIOP over IIOP 1.0 used between Orbix 6.1 and Orbix 3.
69251	Orbix 6.1 Java client to C++ server interoperability issue. Orbix 6.1 Java client can get MARSHAL exceptions when Orbix 6.1 for C++ returns a large (fragmented) reply.
69250	Orbix 6.1 notification service leaks memory and handles.
69248	Typecode marshalling problem between Orbix 3.3.x/Orbix 6.1 and JacORB 1.4.1.
69232	Orbix COMet's `ORB.Narrow()` only works if type to narrow to is prefixed with "`::`".
69207	Orbix 6.1 Service Pack 1 itconfigure bug: `com.iona.cfg.deploy.orbix.OrbixEntityAdapter` is not usable.
69180	Orbix 6.x Java processes fail to start in multihomed machines.

Bug	Description
69177	Orbix 6.1 does not enforce correct port range for `corbaloc` URLs.
69170	In Orbix 6.1 Service Pack 1, `itconfigure` crashes when trying to add a node daemon with the `-multihome` flag.
69163	Error reported in the generated boot script in Orbix 6.1 on IRIX.
69161	Calling `orb.SetOrbName` followed by `orb.RunningInIde` in VBA applications might cause crash in Orbix COMet 6.1 Service Pack 1.
69126	Orbix 6.1 Runtime Only install, which has been installed from CD, has a problem upgrading to Orbix 6.1 Service Pack 1.
69116	COMet VB application might not shut down properly with `COMet:Config:COMET_SHUTDOWN_POLICY = "Implicit"`.
69115	Licenses not accepted with JDK 1.4.2 on Windows 2003 server.
69109	Registering the Orbix services as Windows services is broken in Orbix 6.1 Service Pack 1.
69104	Binding error when java client loading the Generic Security Plug-in (GSP) calls Orbix 2.3.x server.
69101	Null pointer exception in the extended is2 demo if configuration changed in 6.1 Service Pack 1.
69095	In Orbix 6.1.x, services fail to start on machine reboot.
69092	COMet VB client might crash when being run inside a debugger.
69085	`IT_TLS_API::TLSCredentials::get_x509_cert()` not implemented for own credentials.
69071	Orbix 6.1 Service Pack 1 for HPUX install missing libraries.
69068	OrbixRemoting needs another method to obtain interface if type ID is `IDL:omg.org/CORBA/Object:1.0`

Bug	Description
69065	`COMet:Debug:MessageLevel` not used within a scope.
69046	Orbix 6.1 Service Pack 1 command-line `link` option does not work.
69026	ASP 6.0 Service Pack 3 `NullPointerException` in `ProfileEndpointImpl`.
69019	Value of `plugins:pss_db:envs:<env-name>:lg_max` does not get used.
68985	The order in which COMet tries to contact the IFR is incorrect.
68972	ASP 6.0 Service Pack 3 J2EE classloader cache—old versions are not removed from cache when new version of EAR file is deployed.
68900	Potential race condition on connections causing sporadic `ATLI2_IOP:CONNECTION_CLOSED_GETTING_SEND_BUFFER` exceptions.
68862	Attempting to create a linked domain across different DNS domains fails.
68842	IDL struct types mapping to Java does not follow CORBA initialization specifications.
68695	In Orbix 6.1, ASP 6.0 Service Pack 3 and ASP 5.1 Service Pack 2, when AMI is used for invocations, CORBA timeouts do not occur when server is suspended.

Bugs Fixed in Orbix 6.2 Service Pack 1

The following bugs have been fixed in Orbix 6.2.1:

Bug/SR	Description
60695	'Find Objects' dialog window 'Ok', 'Cancel' buttons not mapped to 'Enter', 'Esc' keys.
64827	The ts2tlb tool returns an error when the IDL file contains a module that contains 'const' parameters

Bug/SR	Description
67615	IDL/Java compiler supports long long type, but only allows it 32 bits
68624	Artix designer does not map the targetNamespace to package names
68900	Potential race condition on connections causing ATLI2_IOP:CONNECTION_CLOSED_GETTING_SEND_BUFFER exceptions sporadically
68956	server_address_mode_policy:publish_hostname does not work for https
69156	can not call remote transient object if client is running same PID as server
69216	itadmin process kill -signal doesn't seem to send the correct signal
69261	Per request load balancing in Orbix6.x
69277	Per client activation in Orbix6.x
69333	itconfigure should allow to set up a domain where the Orbix services only listen on one particular network card, instead of listening on all local interfaces.
69493	node daemon core dumping due to unexpected exception being thrown in IT_ND_ProcessRegistryImpl::activate_endpoints
69497	Returning large data in IDL out parameter back to secure client that uses MS-CAPI results in a COMM_FAILURE exception
69508	.NET connector Activator.GetObject() cannot handle some corbaloc URL's
69532	ART C++ POA randomly generated section of the Object Key is not truly random for Transient POAs
69541	Orbix 6.1.1 and 6.0.1 clients leak memory when they time out before the server on Solaris. replies back.

Bug/SR	Description
69566	ASP Java's active connection management feature is inconsistent with the C++ version of the ORB
69580	Enhance Orbix6.x to allow a mid-tier server to set SSO credentials on an outgoing call
69583	itadmin crashes on exit querying the locator if the ZIOP plugin has been configured for everything in the domain
69593	C++ CSIv2Client interceptor will authenticate itself when it is configured not to
69605	The PacingInterval does not work correctly after several days running
69606	COMet needs to cache fully scoped interface names to reduce IFR network traffic
69622	If client is configured to use CSIv2 identity assertion but no identity has been set, it causes a NullPointerException inside the csi plugin
69628	server with persistent poa can't start internal orb with just -ORBconfig_domains_dir (needs iona.properties or -ORBconfig_dir)
69631	nullpointer exception in is2 demo if config changed to not send and receive SAML data
69645	ART TLS configuration should allow users to choose multiple protocols
69646	GSP plugin cant contact IT_Login with a corbaloc on Orbix6.2
69664	iiop_tls memory leak when plugins:iiop_tls:incoming_connections:soft_limit is set
69668	Incorrect casting hides a native Java exception with a ClassCastException in the Orbix Java skeleton code
69672	default current directory for "itadmin process create" fails in node_daemon "error 183: Cannot create a file when that file already exists."

Bug/SR	Description
69674	incorrect error messages in SecurityServerResource.properties of IS2
69677	Calling perform_work() from within a servant code serviced bya single-thread model POA broken in Orbix6.1
69697	"itadmin ifr" fails if corbaname URL is used for the IFR initial reference in configuration
69705	Orbix Java NIO lockup in reserve_bandwidth
69710	ASP/Orbix Java leaves threads behind after ORB::shutdown(true) if an invocation has been made
69716	Programmatically setting the received SSO token on outgoing calls results in ArrayIndexOutOfBoundsException being raised after 10 operations
69727	itconfigure - Installing an empty client domain with "allow secure communication" only
69729	addition of command line options to idlgen to specify the operation or attribute accessor that is to be executed.
69732	idlgen generated code from idl created using wsdltocorba does not build complaining about references to a non generated class
69733	Java code generated by idlgen using the `java_poa_genie.tcl` genie generates bad test data for string arguments.
69750	Orbix6.1.1 .NET Connector, could not find the corresponding .NET Type for the returned CORBA object (when sequence is returned
69778	tls client using schannel hangs if no certificate is available to meet constraints
69779	Passing a 0-length array of Policy objects and using SET_OVERRIDE to PolicyCurrent::set_policy_overrides doesn't clear the existing policies
69800	COMet IT_Marshall exception

Bug/SR	Description
69809	node daemon reports process as active after it has exited - continuation of 69307
69829	TLS schannel client cannot communicate with z/OS 1.6 running ASP 6
69833	Localising a descriptor with more than one profile
69839	The Orbix6.0.3 appserver can raise NullPointerException if beans are accessed concurrently from a number of clients
69854	interface containing long long causes typestore error in COMET6.x
69887	Locator crash due to unhandled exception thrown from within IT_LOC_EndpointReplicaGroup::RequestDispatcher::execute work item
69971	Intermittent hang during TLS handshaking when communicating with z/OS 1.6
70003	Java CSIV2 enabled client not using address list in TLS_SEC_TRANS component
70006	iordump utility does not parse the csiv2 component properly
70008	Java implementation of the CSIv2 protocol permits replies from a CSIv2 enabled server even if the server did not send a CSIv2 response.
SR# 272258	Performance issue; authenticate(realm, userName, password) returns all realms

Note on Bug 69732

Java code generated by idlgen using the `java_poa_genie.tcl` genie imported types defined in OMG modules from package `<package_name>` when option `-jP <package_name>` was used, and hence would not compile. The fix imports types in such modules from the `org.omg` package. The list of modules is configurable (see Appendix A in the CORBA Code Generation Toolkit Guide) and contains all OMG modules by default. Also, `build.xml` files generated by this genie always included instructions to idl compile any OMG idl files (apart from `orb.idl`) that were included in the idl files passed to the genie. This is not necessary and is now avoided. The old behavior can be restored by setting configuration option `default.java_genie.no_idl_compile` to a list containing one element: `["orb.idl" ]` (see Appendix A in the CORBA Code Generation Toolkit Guide).

Note on Bug 70008

Up until Orbix 6.2.1, a client using the Java implementation of the CSIv2 protocol permitted replies from a csiv2-enabled server even if the server did not send a csiv2 response. In Orbix 6.2.1 a new variable has been introduced in the Java plugin to overcome this issue.

`plugins:csi:allow_csi_reply_without_service_context`

It can be set with a boolean value, true or false.

If it is set to false then the client will have strict checking on the reply from the server. If there is no csiv2 component to the reply a NO_PERMISSION exception with a minor code BAD_SAS_SERVICE_CONTEXT will be thrown by the client.

If it is set to true, then the client will get the reply from the server and not issue any warning even if the reply didn't contain a csiv2 component (not recommended).

By default the value will be set to true for backward compatability with domains deployed prior to Orbix 6.2.1 and servers deployed prior to Orbix 6.2.1.

New domains deployed with Orbix 6.2.1 will have the variable set to "false" in configuration.

Enhancements in Orbix 6.2

The following enhancements have been added in Orbix 6.2:

Enhancement	Description
69353	The `AuthenticatedPrincipal` object should be cached instead of the SAML response string, as a result of an authentication process at iS2.
69175	Orbix to allow null strings to be marshalled. For this enhancement to work you must set the `plugins:codeset:interop_allow_null_strings` configuration variable to `true`. See the *Configuration Reference Guide* for more details.
69130	Provide ability to restart a failed process without any `itadmin` commands.
69044	There is no way to deploy a node daemon with `itconfigure` when using the `-link` option from the command line.
68951	Please enhance the Orbix 6.x products to include the MFA commands to interact with the mainframe adapters.
68717	Should be able to configure Orbix 6.0 Service Pack 3 to use a third-party certificate store.
68597	Orbix 6.1 is missing Single Sign-On (SSO) demo.
12000690	ASP 5.1 does not provide usable dynamic reconfiguration of IT_GIOP logging levels.

Enhancements in Orbix 6.2 Service Pack 1

The following enhancement has been added in Orbix 6.2 Service Pack 1:

Enhancement	Description
69261	Per Request Load Balancing
69393	Enable locator to start up under a heavy client load

Per Request Load Balancing

The existing locator load balancing is performed on a per-client ORB basis therefore once a binding to a replica has been established all requests from that ORB use the initial binding. The enhancement allows the user to select an option that will allow load balancing to occur within the ORB, on a per request basis.

To activate per request load balancing set the policy in the configuration file as follows:

```
policies:per_request_lb = "true"
```

Enable locator to start up under a heavy client load

When one attempts to bring up an Orbix server in an environment where a number of clients are already alive, in possession of persistent IORs and continuously trying to invoke on it, it fails to start.

A new message-level interceptor plugin has been introduced in the locator to deal with this.

The plugin closes the connection on locator requests from hosts other than those specified. It will do this until a node daemon has registered - at this point the filter is switched off. The clients need to be able to handle the `CORBA::Exception` as a result of the connection being closed.

To configure the interceptor:

```
plugins:connection_filter:shlib_name = "it_connection_filter";
```

Example:

```
# Add the connection filter to the GIOP message_server_binding_list
   plugins:giop:message_server_binding_list = ["BiDir_GIOP",
   "FILTER+GIOP", "GIOP"];
   # Add the connection filter to the locator orb plugins list
   orb_plugins = ["local_log_stream", "iiop_profile", "giop",
   "connection_filter", "ots", "iiop"];
   # enable the interceptor
   plugins:node_daemon:registration:required = "true";
   # Accept connections from these hosts
```

```
plugins:connection_filter:address:list = ["10.2.2.127"];

# Optional
# Limit the number of threads that are getting created in the
locator - you don't have to do this but it could prevent core dumps
thread_pool:high_water_mark = "200";

# See what the filter is doing
event_log:filters = ["IT_POA_LOCATOR=*", "IT_LOCATOR=*",
"IT_PSS_DB=INFO_HIGH+WARN+ERROR+FATAL", "IT_CONNECTION_FILTER=*"];
```

Type support in COMet 2000

There have been some changes made in Comet2000 with regard to how the unsupported types `const` and `long long` are handled.

In previous versions if you tried to load an idl into the typestore in COMET if it contained either the token ***const*** or ***long long*** the idl would not be processed and the command would exit with an error .

Now the typestore loads in the idl but ignores the unsupported types and prints out a warning indicating that these tokens are ignored.

Likewise when preforming operations on the typestore for example ts2idl or ts2tlb the unsupported types are ignored , a warning is printed and the command continues with processing the remainder of the interface .

Documentation Enhancements

The Orbix Deployment Guide explains everything you need to know about configuring and deploying an Orbix domain. For example, how to run the **Orbix Configuration** tool, the contents of the generated deployment descriptor, and advanced topics such as domain migration. Some of this material was contained in the Administrator's Guide in previous Orbix releases.

Migrating and Upgrading from Earlier Versions

Migrating from ASP 5.1

If you are migrating from ASP 5.1 to Orbix 6.2, see the Orbix Migrating from 5.1 to 6.2 Guide.

Migrating from Orbix 3.3

If you are migrating from Orbix 3.3 to Orbix 6.2, see the Orbix Migrating from 3.3 to 6.2 Guide.

Upgrading from Orbix 6.x

Orbix 6.2 also has in-built support for migrating configuration domains created with ASP 6.0 and Orbix 6.1. This allows you to quickly upgrade a production installation without the need to manually recreate persistent data such as registered processes, orb names, and so on. For more information, see the Orbix Deployment Guide.

In addition, changes have been made to the semantics of the `IT_Config::Configuration::get_list` and `IT_Config::Configuration::get_string` operations. For more detail, see the Orbix Programmer's Reference Guides.

Platforms/Features Not Supported in Next Release (Orbix 6.3)

From Orbix 6.3, the IONA JMS implementation and the JMS/Notification bridge will not be included in the Orbix product. The following table details the changes that are scheduled for Orbix 6.3:

Operating System	C++ Compilers	Java Compilers	To be Replaced by
All operating systems		JDK 1.3.1	JDK 1.5
Sun Solaris 10	Forte 6.2		Sun Studio 10
	Visual Age 6.0		XL C/C++ 7.0
Microsoft Windows 2000			Microsoft Windows 2003
	Visual C++ 7.0		Visual C++ 7.1

Reporting Problems

Contact customer support at http://www.iona.com/support/contact/

Other Resources

- Knowledge Base articles (`http://www.iona.com/support/knowledge_base/index.xml`) provide a database of practical advice on specific development issues, contributed by IONA developers, support specialists, and customers.
- IONA University (`http://www.iona.com/info/services/ps/`) delivers practical and insightful courses that cover technical and product issues, as well as standards-based best practices gleaned from real-world projects.
- IONA Professional Services (`http://www.iona.com/info/services/consulting/`) IONA offers up-front support contracts with a duration ranging from one to five years for Orbix 6.2. With more customers and more systems in production than any other CORBA vendor, IONA offers the highest quality CORBA support in the industry.

  In addition, IONA's Professional Services and our Consulting Partners provide experienced developers, architects and project managers to assist with the architecture, design, development, integration, rollout, support and optimization of your Orbix 6.2 applications. No matter what your integration challenges are, IONA consultants can play any number of roles, on both short and long-term engagements, to help you get the most out of Orbix 6.2.
- IONA security bulletins are available as part of our customer warning system. To receive these bulletins, please subscribe to the *`security-alert@iona.com`* mailing list.

  To subscribe send an email to `listserver@iona.com`. Leave the email **Subject** field blank and, in the body of the email, type:

  subscribe security-alert <your email address>

  To unsubscribe do the same, but type unsubscribe in the body of the email.

  Note: Please do not try to post queries to this email alias; it has not been set up to receive queries.