Orbix 6.3.7 Release Notes

These release notes contain information about the Orbix 6.3.7 release from Micro Focus. They contain information that might not appear elsewhere in the documentation. Read them in their entirety before you install the product.

Orbix 6.3.7 has been rebranded as a Micro Focus product.

New Features

Orbix 6.3.7 includes the following new features:

- TLS/SSL over NIO
- Load-balancing policy

TLS/SSL over NIO

The Orbix 6.3.7 Java runtime now supports TLS/SSL secure connections over Java's New I/O (NIO).

Load-balancing policy

A new time-based load-balancing policy has been introduced. You can set a timeout to modify the existing CLIENT_LOAD_BALANCING_POLICY_ID policy. In a situation where multi-threaded clients connect to replicated, load-balanced servers the client connections are taken from the client's binding pool. When a server replica goes down, the relevant binding in the pool is updated to point to the next available server replica. Refreshing the list of available bindings, at the interval defined by the new configurable timeout, ensures that when a server replica is restarted it is listed as available in the client's binding pool. This helps ensure that the load is balanced across all the available server replicas.

CORBA Compliance

Orbix 6.3 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

Platforms and Compilers

For the latest information on supported platforms and compilers, see the Orbix Supported Platforms page.

Migration from Previous Versions

To upgrade to Orbix 6.3.7 from existing Orbix 6.3.x installations:

- Back up existing installations before you upgrade to Orbix 6.3.7.
- Go to the Orbix 6.3.x directory and run the Orbix 6.3.7 installer. The Orbix installer overwrites the existing version.
- If your existing Orbix deployment is configured to use the Baltimore security toolkit or the Baltimore-based Key Distribution Mechanism, refer to the instructions in Migrating away from Baltimore security toolkit page 2..

For details on installing Orbix 6.3.x service packs, see the *Orbix Installation Guide*. For details on migrating from earlier Orbix versions, see the migration and upgrade documentation at https://supportline.microfocus.com/productdoc.aspx.

Migrating away from Baltimore security toolkit

The Baltimore security toolkit has been deprecated since Orbix 6.3.4 and is removed from Orbix 6.3.7. If your existing Orbix installation was configured to use the Baltimore security toolkit, you must now reconfigure it

Migration from Baltimore security toolkit deployments to OpenSSL / JSSE security toolkit deployments

If your existing Orbix deployment was configured to use the Baltimore security toolkit, the following configuration variables will need to be modified:

```
# Baltimore security toolkit
initial_references:IT_TLS_Toolkit:plugin =
   "baltimore_toolkit";
policies:mechanism_policy:protocol_version = ["TLS_V1",
   "SSL_V3"];
plugins:atli2_tls:use_jsse_tk = "false";
```

To enable the use of the OpenSSL security toolkit and the Java JSSE/JCA security toolkit, the relevant configuration variables must be changed to the following values:

```
# OpenSSL and JSSE security tookit
initial_references:IT_TLS_Toolkit:plugin =
   "openssl_toolkit";
policies:mechanism_policy:protocol_version = ["TLS_V1_2",
   "SSL_V3"];
plugins:atli2_tls:use_jsse_tk = "true";
```

Migration of Key Distribution Mechanism (KDM) to use OpenSSL

The deprecated Baltimore security toolkit has been removed in Orbix 6.3.7. When upgrading previous Orbix installation to Orbix 6.3.7, domains which use the Baltimore based Key Distribution Mechanism will need to migrate to the OpenSSL based Key Distribution Mechanism.

If your domain does not use the KDM or you are using a 64-bit Orbix installation on Windows, then you do not need to take any manual steps to upgrade to Orbix 6.3.7 and you can disregard the rest of this section.

You can determine whether your pre-6.3.7 Orbix deployment is using a Baltimore-based KDM by checking the value of the plugins:`kdm:shlib_name` and `plugins:kdm_store:shlib_name` variables:

Baltimore-based KDM:

```
plugins:kdm:shlib_name = "it_kdm_server"
plugins:kdm_store:shlib_name = "it_kdm_store_pss_r"
```

OpenSSL-based KDM:

```
plugins:kdm:shlib_name = "it_kdm_server_openssl"
plugins:kdm_store:shlib_name = "it_kdm_store_pss_r_openssl"
```

To migrate your Baltimore-based KDM database to the OpenSSL-based KDM format, you will need to follow these steps:

- Prior to upgrading to Orbix 6.3.7, use the `itadmin` tool in your existing Orbix installation to gain a list of the existing KDM database entries. There are two types of entry, orbname/passphrase pairs and checksums.
  - To get the list of orbnames that you will need to re-enter the passphrase for in the OpenSSL-based KDM database, use the command:

    ```
    itadmin kdm_adm list
    ```

  - To get a list of the checksums that you will need to re-enter in the OpenSSL-based KDM database, use the command:

    ```
    itadmin checksum list
    ```

- Keep a record of this data. Have the passphrase associated with each orbname ready.
- Upgrade to Orbix 6.3.7 following the instructions in the *Installation Guide*.
- After upgrading to 6.3.7, the KDM database will need to be backed up and moved to a different location, in order for the locator to start up correctly. If the KDM database is not moved, attempting to start the locator will result in an `IT_KDM:KDM_DATABASE_CORRUPT` error.

  The KDM database file can be found at this location:

  ```
  $DATA_DIRECTORY/<domain-name>/dbs/locator_priv/IT_KDM_St
     oreImpl_KDMDataHomeImpl_1_0
  ```

  In a default installation of Orbix, this database file will be:

  ```
  $IT_PRODUCT_DIR/var/<domain-name>/dbs/locator_priv/IT_KD
     M_StoreImpl_KDMDataHomeImpl_1_0
  ```

- After moving the Baltimore-based KDM database file, you will be able to start the locator and re-populate the OpenSSL-bsed KDM database with the configuration data collected in an earlier step by using the `itadmin` tool.

For further details and examples of how to manage passphrases and checksums using the itadmin tool and the KDM, please refer to the chapter *Automatic Activation of Secure Servers* in the Orbix security guide.

Known Issues

Orbix 6.3.7 includes the following known issues:

- Deployment problem on Windows 7 or Windows 2008 R2 VM on VMWare
- client_address_mode_policy on Windows Vista/Windows 7
- Actional integration
- Supported platforms for Actional
- Instrumented CFR domain without security service
- Spaces in install path and itant
- Orbix Java services on Linux with 64-bit JDK
- Secure CFR domain with replicated services
- Compiling 64-bit C++ applications

Deployment problem on Windows 7 or Windows 2008 R2 VM on VMWare

You might encounter an intermittent failure to deploy services on virtual machines with only 1 CPU. This problem does not occur when the virtual machine has 2 or more CPUs.

client_address_mode_policy on Windows Vista / Windows 7

Errors occur on Windows Vista or Windows 7 when using the `policies:iiop:client_address_mode_policy:local_hostname` configuration variable.

When `policies:iiop:client_address_mode_policy:local_hostname` is set to "localhost", the client ORB resolves the IP address and binds it to 127.0.0.1.

If the address published by the server is the actual hostname or numeric IP of the server, then the connection fails and the system displays an error message "Network is unreachable" with a Winsock error value 10057.

If `policies:iiop:client_address_mode_policy:local_hostname` is set to 10.X.X.X or the actual hostname and if the address published by the server is 127.0.0.1, the connection fails and the system displays an error message "Cannot assign requested address" with a Winsock error value 10049.

To resolve the problem, you must set the `policies:iiop:client_address_mode_policy:local_hostname` configuration variable to the address published by the server.

Actional integration

By default, the CORBA Telecom Logging services are not instrumented when you use the **Orbix Configuration** tool to enable integration with the Aurea Actional® Application Performance Monitoring system. However, integration with these services can be configured using the `enable_actional.tcl` script. Integration between Orbix performance logging and Actional is not supported. See also Instrumented CFR domain without security service.

Supported platforms for Actional

Integration with the Aurea Actional® Application Performance Monitoring system is not supported by Orbix for Microsoft Windows VC11 32-bit or VC11 64-bit editions.

Instrumented CFR domain without security service

A configuration repository-based domain that has been fully instrumented with Actional, but does not include an Orbix security service, might have an issue when some instrumented services (for example, the naming service or node daemon) are started.

The following error might be reported during service startup:

```
IT_Core:ON_POSSIBLE_SERVER_BINDING
```

Windows platforms may report this error as a system exception during service startup. This issue is due to a bug in the configuration generation tool, and will be fixed in a patch. Please contact your Technical Support representative for download details of this patch.

As a workaround, use the following command to fix your domain configuration for each affected service. When this command is run, the service will start successfully:

```
itadmin InstallDir/asp/6.3/bin/enable_actional.tcl
   iona_services.Service.Hostname
```

For example:

```
itadmin InstallDir/asp/6.3/bin/enable_actional.tcl
   iona_services.node_daemon.my_host_name
itadmin InstallDir/asp/6.3/bin/enable_actional.tcl
   iona_services.naming.my_host_name
```

Spaces in install path and itant

If your Orbix installation path contains spaces, and you use the `itant` tool to build the Java demos, the following message might appear in the console output:

```
C:\Program%20Files\Progress\Orbix\asp\6.3\demos\corba\demo.xml
   could not be found
```

This is a benign message and can be ignored. The Java demos build successfully.

Orbix Java services on Linux with 64-bit JDK

On Linux, with a 64-bit JDK, you must also install a 32-bit JDK to use Orbix Java services (for example, management, security, and trader services). This is because Orbix Java services run in a 32-bit JVM. For example, after you have installed 32-bit JDK, you can set up your environment as follows:

```
export JAVA_HOME_32=~/jdk1.6.0_16
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$JAVA_HOME_32/jre/lib/
   i386/server
```

Secure CFR domain with replicated services

In a secure configuration repository (CFR)-based domain with replicated Orbix services, CFR replica sets can not be automatically shrunk. This issue does not occur in an insecure CFR-based domain. If you have to remove CFR replicas in a secure CFR-based domain, please contact Orbix technical support.

Compiling 64-bit C++ applications

When compiling 64-bit applications with the C++ Sun Studio 12 Update 2 compiler on a Solaris x86 platform, there may be issues relating to compiling certain demos delivered with Orbix. The issue relates to a known compiler bug in the C++ compiler. Oracle is aware of this issue, and as a workaround suggests compiling the code with the `-O1` flag instead of using the debug `-g` flag.

Resolved Issues

The resolved issues that customers have reported are listed in this section. The numbers that follow each issue are the Reported Problem Incident number followed by the Customer Incident Numbers (in parentheses). RPIs that have numbers only (and no text) are included to confirm that the RPIs have been fixed, since no further information is required.

- 599714
- 599887
- 1089252 (2643375)
- SSL is now supported in combination with the NIO IP transport.

  1089308 (2646582)
- Windows Server 2012 is now supported.

  1089350 (209526)
- Windows 8 is now supported.

  1089392 (2641499)
- An exception could be thrown from the ORB if multiple threads tried to invoke on the ORB.string_to_object() method, passing in a corbaloc url. The method responsible for unmarshaling the corbaloc url into an object reference was not thread safe, so a race condition could occur when it was invoked by multiple threads. This has been fixed.

  1089460 (2647987)
- 1090885 (2660691)
- Added the configuration variable `plugins:orb:max_unbounded_string_size`. This enables the customer to set the maximum size of an unbounded string in megabytes.

  1090914 (228900)
- A new time-based load-balancing policy has been introduced. It enables the client side to configure a timeout for when proxy load-balancing is used. When the configured timeout expires the client proxies will have the ORB's internal binding lists refreshed, so they are made aware of any changes to server replicas. Any subsequent client requests will then be routed to the next available server replica.

  1091275 (2666968)
- If a C++ IDL sequence constructor ran out of memory, it crashed with a segmentation violation. Now, a COBRA::NO_MEMORY C++ exception is thrown.

  1091714 (2670248)

- The Orbix 6 demo SSL Certificates were due to expire in June 2014, so any customers still using them will face issues. This release contains updated versions of these SSL Certificates.

  1094448 (2700365)
- Core dump when starting Orbix 6.4.6 Notification Service in Solaris 11.

  1095082 (2782827)

Other Resources

The following additional resources are available:

- For the latest information on supported platforms and compilers, see the Orbix Supported Platforms page.
- The most up-to-date versions of Orbix technical documentation are available at:

  https://supportline.microfocus.com/productdoc.aspx

  The Orbix Knowledge Base is a database of articles that contain practical advice on specific development issues, contributed by developers, support specialists, and customers. This is available at: http://community.microfocus.com/microfocus/corba/orbix/w/knowledge_base/
- Contact Micro Focus technical support at:

  http://www.microfocus.com