Orbix 6.3.8

Release Notes

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

http://www.microfocus.com

2015-12-22

Contents

Orbix 6.3.8 Release Notes

These release notes contain information about the Orbix 6.3.8 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.

New Features

Orbix 6.3.8 includes the following new features:

- Support for SHA-256
- 64-bit Services
- SSL v3 disabled

Support for SHA-256

Support for certificates that use SHA-256 has been added to Orbix 6.3.8. See RPI 1099542 (2821543) for details.

64-bit Services

Orbix 6.3.8 includes 64-bit services for all mixed mode kits. Previous releases of Orbix 6 deployed only 32-bit services in kits that had both 32-bit and 64-bit binaries; that is, in Solaris SPARC (except with JDK 8), Solaris x86, Linux, HP-UX PA-RISC and HP-UX Itanium 64.

In Orbix 6.3.8, if the deployer runs with a 64-bit JVM it will deploy 64-bit services. To do this:

- On Solaris SPARC, Solaris x86, HP-UX PA-RISC and HP-UX Itanium 64, you need to run:

  ```
  itconfigure -jvm64
  ```

  This selects the 64-bit JVM.
- On Linux, the JDK supplied is not mixed mode. Therefore, you need only run `itconfigure` with `JAVA_HOME` set to a 64-bit JDK and Orbix will deploy with 64-bit services.

Note that:

- The JDK version 8 supplied with Solaris SPARC is 64-bit only, so always deploys 64-bit services whether `-jvm64` is specified or not.
- Any 32-bit only kit (such as Windows 32-bit and AIX 32) is not affected.

SSL v3 disabled

Starting with Orbix 6.3.8, Orbix 6 as delivered has the SSL v3 security protocol disabled by default. SSL v3 can still be configured for backwards compatibility with older servers; however it should be noted that SSL v3 is susceptible to the POODLE exploit, and where possible customers should upgrade to the newer and more secure TLS protocols.

By default Orbix 6.3.8 supports the following TLS protocols:

- TLS v1.0
- TLS v1.2

To enable SSL v3, you must add "`SSL_V3`" to the following configuration variables:

- `policies:iiop_tls:mechanism_policy:protocol_version`
- `policies:https:mechanism_policy:protocol_version`

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 6.3.8 from existing Orbix 6.3.x installations:

- Back up existing installations before you upgrade to Orbix 6.3.8.
- Go to the Orbix 6.3.x directory and run the Orbix 6.3.8 installer. The Orbix installer overwrites the existing version.

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.

Known Issues

Orbix 6.3.8 includes the following known issues:

TLS 1.2 with IBM JDKs

IBM Java, starting with versions 7 and 8, forbids the use of certificates that are signed with MD5 (MD5WithRSA). This is not an issue with other JCA implementations (Oracle and HP), nor with lower versions of the TLS protocols.

This excerpt from the TLS 1.2 specification does signify that MD5 should no longer be considered a safe hashing algorithm:

> ***MD5***
>
> *MD5 [MD5] is a hashing function that converts an arbitrarily long data stream into a hash of fixed size (16 bytes). Due to significant progress in cryptanalysis, at the time of publication of this document, MD5 no longer can be considered a 'secure' hashing function.*

Micro Focus highly recommends that any certificates used in secure Orbix applications that are signed with an MD5 digest signature are regenerated to use at least a SHA-1 digest signature.

Disk Space Checking During Installation

When installing on a UNIX platform, a warning message might be issued indicating there is not enough space on the file system to install Orbix. This is due to an issue with InstallAnywhere, which may not be checking the disk space of the intended file system. Check that the file system does indeed have sufficient space to install Orbix, then set the following environment variable and re-run the installer:

```
export CHECK_DISK_SPACE=OFF
```

Invalid Unzip During Installation

When installing on a UNIX platform, a message similar to the following may be issued:

```
microfocus_orbix_6.3.8_<platform>.bin[2827]: unzip: not found
Invalid unzip command found
```

This is due to a known issue with InstallAnywhere. This message can be ignored.

Oracle Solaris Studio 12.4 compiler

Oracle Solaris Studio 12.4 compiler is not supported with Orbix 6.3.8. A compiler issue was uncovered while certifying Orbix 6.3.8 with Studio 12.4. The compiler issue relates to an inconsistent behavior in mangling symbol names between Studio 12.4 and earlier compiler versions. Micro Focus is working with the compiler vendor towards a resolution of this issue.

Micro Focus advises customers to refrain from using Oracle Solaris Studio 12.4 with Orbix 6.3.8 until this issue is resolved.

Java 8 Compatibility when Deploying Security Enabled CFR Domains with the IS2 Service

There is a Java 8 compatibility issue when deploying Secure and Semi-Secure CFR deployments with the IS2 service. Starting with Java 8 update 60, Oracle have dropped support for the RC4 ciphersuite. This can result in a situation where the `itconfigure` GUI deployment tool will give an error such as "`Failed to narrow CFR reference`".

There are two workarounds for this issue:

1. Modify the `java.security` configuration file in the Java 8 installation `<jre-home>/lib/security/java.security` by removing any reference to "`RC4`" from the Java property `jdk.tls.disabledAlgorithms`.
2. Modify the `tls.xml` file that the `itconfigure` deployment tool parses when deploying a secure domain. This involves replacing the following xml nodes:

```
<configData>
  <dataId>policies:mechanism_policy:ciphersuites</dataId>
  <dataType>list</dataType>
  <dataValue>RSA_WITH_RC4_128_SHA</dataValue>
  <dataValue>RSA_WITH_RC4_128_MD5</dataValue>
</configData>
```

   Replace each occurrence of the xml nodes with the following:

```
<configData>
  <dataId>policies:mechanism_policy:ciphersuites</dataId>
  <dataType>list</dataType>
  <dataValue>RSA_WITH_RC4_128_SHA</dataValue>
  <dataValue>RSA_WITH_RC4_128_MD5</dataValue>
  <dataValue>RSA_WITH_DES_CBC_SHA</dataValue>
  <dataValue>RSA_WITH_3DES_EDE_CBC_SHA</dataValue>
</configData>
```

After you have made either of these changes, Micro Focus recommends that the `itconfigure` tool is restarted, and any remaining services that may be left around by the failed deployment attempt are terminated. You can then re-run the `itconfigure` tool.

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.

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.
- Microsoft Windows VC12 32-bit or VC12 64-bit editions.

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\Micro%20Focus\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.

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.

Issues resolved in this Service Pack

This section includes issues that are resolved for the first time in this Service Pack.

- A fix for the `itconfigure` tool shows the correct list of licensed services that can be added to a domain.

  601167

- Fixes an issue where strings of `max_unbounded_string_size - 1` were not being allowed.

  608182

- The documentation for `max_unbounded_string_size` has been updated in the ***Orbix Configuration Reference***.

  608290

- The idl file `messaging_admin.idl` was not being packaged.

  614738

- The Unix installers were setting two environment variables:
  - `IT_PRODUCT_DIR`
  - `JAVA_HOME`

  This behavior is required for the Windows installers. However on Unix the installer was writing the environment variables into the user's Bourne shell `.profile` initialization script.

  The Unix installer no longer writes to the `.profile` script.

  614953

- When a TLA client issued an ORB `shutdown()` call using NIO, a TLS server would generate an error about a read failure.

  RPI 1096386 (2791792)

- 1097123 (2796840)

- Support for SHA-256 has been added to Orbix 6.3.8. Support for the following cipher suites has been added:

  ```
  RSA_WITH_AES_128_CBC_SHA
  RSA_WITH_AES_256_CBC_SHA
  RSA_WITH_NULL_SHA256
  RSA_WITH_AES_128_CBC_SHA256
  RSA_WITH_AES_256_CBC_SHA256
  ```

  RPI 1099542 (2821543)

- In Orbix 6.3.8 for C++, the unbounded string size limit has been removed, so that unbounded strings are fully unbounded in nature.

  RPI 1100822 (2831620)

- The client-side leasing plug-in no longer crashes after failing to renew a lease with a server.

  RPI 1101831 (2840529)

Issues resolved in previous HotFixes

This section includes issues that were fixed in HotFixes to Orbix 6.3 SP7, and are now incorporated into SP8.

- An Orbix 6.3.7 application could not extract the x509 certificate from credentials when using the OpenSSL toolkit. The call to `get_x509_cert()` returned `null`.

  1095912 (2699376)

- The TLS server no longer leaks memory if a handshake fails.

  RPI 1096288 (2794922)

- When compiling any IDL-generated C++ header file before Orbix 6.3.7 HotFix 02, the GCC 4.8.2 compiler included with Red Hat Linux 7 would produce a number of warnings:

  ```
  "access declarations are deprecated in favour of
  using-declarations; suggestion: add the 'using' keyword
  [-Wdeprecated]"
  ```

  RPI 1097202 (2803765); RPI 1097619 (2806615); RPI 1098903 (2814275)

- [Windows only] Orbix C++ no longer fails to create a listener if a socket with the `SO_EXCLUSIVEADDRUSE` socket option is bound within the range specified by the `policies:iiop:server_address_mode_policy:port_range` configuration variable.

  RPI 1097458 (2805898)

- The configuration variable `binding:reuse_client_binding` and the policies `REUSE_CLIENT_BINDING_POLICY` and `DISABLE_REUSE_CLIENT_BINDING_POLICY` are introduced to allow the reuse of established client bindings. The configuration variable `binding:reuse_client_binding` defaults to `false`, meaning that the client bindings established in the original object reference are not reused; but this behavior can be overridden by the policy `REUSE_CLIENT_BINDING_POLICY` at runtime. If the configuration variable `binding:reuse_client_binding` is set to `true`, the behavior can be overridden by the policy `DISABLE_REUSE_CLIENT_BINDING_POLICY` at runtime.

  If `binding:reuse_client_binding` is not configured or is set to `false`, but the policy `REUSE_CLIENT_BINDING_POLICY` is set to `true`, established bindings in the original object reference will be reused. If both `binding:reuse_client_binding` and `REUSE_CLIENT_BINDING_POLICY` are not configured or are set to `false`, no behavior changes.

  If `binding:reuse_client_binding` is set to `true`, and the policy `DISABLE_REUSE_CLIENT_BINDING_POLICY` is not set or is set to `false`, established bindings in the original object reference will be reused. If both `binding:reuse_client_binding` and `DISABLE_REUSE_CLIENT_BINDING_POLICY` are set to `true`, no behavior changes.

  RPI 1098127 and RPI 1099252 (2810331)

- An `itconfigure` of Orbix 6.3.7 on Windows 2012 R2 failed with the message `"Could not find file platform_env_windows server 2012 r2.xml"`.

  RPI 1098360 (2812594)

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