Oracle® Fail Safe

Release Notes

Release 4.2.1 for Microsoft Windows

E66370-02

June 2018

Oracle Fail Safe Release Notes, Release 4.2.1 for Microsoft Windows

E66370-02

Primary Author: Tanaya Bhattacharjee

Contributing Authors: Paul Mead, Janelle Simmons

Contents

1.1 How These Notes Are Organized

The release notes are divided into the following sections:

1.2 Certification Information

The latest certification information for Oracle Fail Safe is available on My Oracle Support at

https://support.oracle.com/

1.3 Installation

Due to necessary changes in the format of Oracle Fail Safe home directory structure, versions before 4.1.0 of Oracle Fail Safe must be deinstalled.

1.4 New Features

The following section provides information about the new features and additions in the Oracle Fail Safe release:

1.4.1 Support for TNS_ADMIN Directory

This release of Oracle Fail Safe adds support for the TNS_ADMIN environment variable to locate the network configuration files `tnsnames.ora, listener.ora,` and `sqlnet.ora.`

1.4.2 Support for Read-Only Database Homes

This release of Oracle Fail Safe supports the use of an Oracle database home that is configured as a read-only.

1.4.3 Ability to Open and Close Pluggable Databases using Oracle Fail Safe Manager

If you use a container database, it is possible to open and close the individual pluggable databases owned by the container database. When closing a database, Oracle Fail Safe will use the normal option, that is, the pluggable database will not close until all database connections have voluntarily terminated. When opening a pluggable database, Oracle Fail Safe provides the ability to open the database in read-only or read-write mode, and the database may open in restricted mode, if desired.

> **Note:**
>
> The container database cluster resource must be online before the Oracle Fail Safe Manager displays any information about pluggable databases owned by the container database.

1.4.4 Oracle Local Groups

This release adds enhanced support of the Oracle local user groups. In previous releases, when adding a database to a cluster group (role), if the operating system authentication was chosen for the authentication method, Oracle Fail Safe would create a local group named `ORA_sid_DBA` on the other nodes in the cluster and it would add the Fail Safe server username to that group. If the `ORA_sid_DBA` local group on the original owner node contained other member entries, those entries were not replicated to the other cluster nodes.

In this release of Oracle Fail Safe when a database is added to a cluster group, if the `ORA_sid_DBA` local group exists, it is copied to the other cluster nodes. Similarly, the `ORA_sid_OPER` group is replicated to other nodes. Fail Safe will not copy any group members that are specific to that node, such as a local user name. It will copy Windows built-in members. For example, the built-in Administrators member will be copied to other nodes.

During cluster validation, Oracle Fail Safe compares the Oracle local user groups on each node in the cluster to determine if they have the same member lists. The specific groups that are verified are:

- `ORA_DBA`
- `ORA_OPER`
- `ORA_homename_DBA`
- `ORA_homename_OPER`
- `ORA_homename_SYSBACKUP`
- `ORA_homename_SYSDG`
- `ORA_homename_SYSKM`
- `ORA_sid_DBA`
- `ORA_sid_OPER`

If a local group does not have identical member lists on all nodes of the cluster, a warning message is issued. Oracle Fail Safe only examines the `ORA_sid_DBA` and `ORA_sid_OPER` local groups for databases that are cluster resources (members of a cluster role).

1.4.5 Event Source Name Changed in Windows Application Event Log

Events that are logged by Oracle Fail Safe in the Windows application event log now show Oracle Fail Safe as the event source. In the previous releases, the event source was OracleMSCSServices.

1.4.6 Password Management

In the earlier Oracle Fail Safe releases, if the Oracle Fail Safe server used operating system authentication when accessing a database, password files were not created when a database was added to a cluster group. If the operating system authentication

was enabled, Oracle Fail Safe Manager could not change the password for the database SYS user account.

In this release, when a database is added to a cluster group, Oracle Fail Safe Manager accepts the password for the SYS user account even when operating system authentication is selected as the authentication method for the Oracle Fail Safe server to use when accessing the database. A password file is created on each node according to the password you provide. Oracle Fail Safe Manager allows the password for the database SYS user account to change.

1.4.7 Databases May Be Opened in Read Only and Restricted Modes

Oracle Fail Safe Release 4.2.1 introduces the ability to open an Oracle database cluster resource using the Read Only open mode or with logins restricted to users with the Restricted Session privilege. The selected mode is used if the database fails over to another cluster node, or if the database resource is taken offline and then brought online using a utility other than Oracle Fail Safe Manager. For example, if a database goes offline and then comes online using the Windows cluster manager utility, it will retain the open mode and restricted settings from the last time it opened using Oracle Fail Safe Manager.

In this release, you can select the Read Only and Restricted Modes when the Oracle Database resource is online or offline:

- When an Oracle Database cluster resource is online, you can select the Read Only or Read Write options on the Select Open Mode page.
- When the Oracle Database cluster resource is offline, you can select the desired options on the Properties page for the resource. When the database is brought online the next time, the previously selected mode is used. The open mode may only be changed on the Properties page if the database is offline. The restricted setting can be changed at any time.

  If the database role is a physical standby, then the Properties page shows the following options which are relevant to a standby database:

  – Read Only
  – Enable real time apply
  – Restricted
  – Enable Is Alive polling

  You can set the database to the Read Only mode and select the real time apply checkbox.

You can also change the database open mode and restricted settings using the PowerShell cmdlets. The following commands will start the database in Read Only Restricted mode:

```
PS C:\Users\admin> $db = Get-OracleClusterResource "Test Database"
PS C:\Users\admin> $db.OpenMode = "ReadOnly"
PS C:\Users\admin> $db.IsRestricted = $true
PS C:\Users\admin> Start-ClusterResource $db.name
```

1.5 Unsupported Features

The following sections provide information about the unsupported features in the Oracle Fail Safe release:

1.5.1 Application Services

Oracle Application Services is not supported in this Oracle Fail Safe release.

1.5.2 Oracle Enterprise Manager 12.1 Agents

Oracle Enterprise Manager Agent is not supported in this Oracle Fail Safe release.

1.5.3 Oracle Automatic Storage Management

Oracle Fail Safe Server does not support Oracle Automatic Storage Management.

1.6 Software Compatibility

Oracle Fail Safe supports automatic clusterwide configuration of highly available databases and applications on Windows server clusters with one, two, or more nodes. This sections includes the following topics:

1.6.1 Oracle Fail Safe Client

Oracle Fail Safe Manager, the client, works with Oracle Fail Safe Server version 3.4.2.4 and later patch sets. Oracle Fail Safe Manager is supported on the following operating systems:

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10

> **Note:**
>
> Windows 7 must have Windows Management Framework 4.0 installed.

1.6.2 Oracle Fail Safe Server

Oracle Fail Safe Server is supported on the software listed in the following table:

Software	Release or Version
Oracle Database (Standard and Enterprise editions)	Oracle Database 11*g* Release 2 (11.2) Oracle Database 12*c* Release 1 (12.1) Oracle Database 12*c* Release 2 (12.2)
Oracle Management Agent	Release 11.2 (A Management Agent release for Microsoft Windows only)
Microsoft Windows Platforms	Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2 Microsoft Windows Server 2016

1.6.3 Windows Server Systems

Oracle Fail Safe Server must be installed on Windows Failover Clusters. It is not supported on non-server systems such as Windows 7 and Windows 8.

1.6.4 32-Bit Server Platforms

This Oracle Fail Safe release is not supported on 32-bit server platforms. Only Oracle Fail Safe Manager is supported on 32-bit client.

1.7 Problems Fixed

This section includes the following problems fixed on Oracle Fail Safe since release 4.1.1.0:

1.7.1 OCIEnvNlsCreate Failed Error When Database 12*c* Not Installed

BUG 20635389

If Oracle Database 11*g* was installed and Oracle Database 12*c* was not installed on all cluster nodes, then any database operations attempted by Oracle Fail Safe would fail with the following error:

```
OCIEnvNlsCreate failed
FS-10999: An internal programming error has occurred
```

The Oracle Fail Safe server did not initialize the runtime environment if Oracle Database 12*c* was not installed on the system.

This problem has been corrected. The Oracle Fail Safe server now initializes correctly, regardless of the Oracle database version installed on the cluster nodes.

The workaround is to install Oracle Database 12*c* on all cluster nodes or downgrade to Fail Safe release 4.1.0.

1.7.2 Modifying Resource Property Fails with FS-10718, 0xD: The data is invalid Error

BUG 20633529

When you attempt to modify a cluster resource common property, such as the "Maximum Restarts" property, it would fail with the following errors:

```
FS-10890: Oracle Services for MSCS failed during the put_data operation
FS-10718: Failed to write the private properties for resource {resource name} in the
cluster
0xD: The data is invalid
```

The Oracle Fail Safe server was attempting to write cluster resource private properties when there were no properties to write. For example, the private property is the text parameter file (pfile) for a database.

The Oracle Fail Safe server no longer attempts to update the resource private properties if there are no changes.

The workaround is to use the Windows failover cluster manager to update the resource common properties.

1.7.3 Startup of Database Cluster Resource Times Out with FS-10727 or FS-10436 Error

BUG 20662316

When starting a database, Oracle Fail Safe would report a timeout error. For example, when verifying a standalone database, you may encounter the following error:

```
0x41D: The service did not respond to the start or control request in a timely
fashion
FS-10436: Failed to start Windows service OracleServiceOFS1
FS-10032: Failed to start the database Test Database
```

When attempting to online a database cluster resource or add a standalone database to a cluster group (role), you may encounter the following errors:

```
FS-10382: NODE1 : Bringing resource Test Database online
FS-10727: Resource Test Database timed out trying to come online
```

In Oracle Fail Safe release 4.1.1 some of the timeout parameters were reduced, making it more likely that a timeout failure would occur.

The database startup timeout parameters have been restored to the values used in previous releases.

1.7.4 Validate Group Fails with an FS-11412 Error

BUG 20662774

If a failover cluster was upgraded to Oracle Fail Safe release 4.1.1 using a rolling upgrade any existing cluster group (role) TNS listeners were considered invalid by the group Validate function. An error similar to the following was returned:

```
FS-10300: Verifying Oracle Net listener resource
OracleOraDB12Home1TNSListenerFslGroupName
FS-11412: The listener OracleOraDB12Home1TNSListenerFslGroupName entry is not found
FS-11414: The TCP address list of listener OracleOraDB12Home1TNSListenerFslGroupName
is incorrect
```

The same error was returned if the TNS listener's cluster resource name was modified. Oracle Fail Safe 4.1.1 derived the listener name from the cluster resource name instead of using the name stored in the resource private properties. This could result in the incorrect name being used for the TNS listener

This problem has been corrected. The listener's name is now fetched from the resource private property which ensures that the correct listener name is used, regardless of the name of the listener cluster resource.

1.7.5 Oracle Fail Safe Manager Fails with Value does not fall within the expected range Error

BUG 20686726

When using the Oracle Fail Safe manager to add an Oracle database to a cluster group, if the "Use operating system authentication" button is checked on the Authentication page and the Next button is clicked, Fail Safe Manager would fail and display the following stack trace:

```
exception message: Value does not fall within the expected range
at Oracle.FailSafe.ResourceDatabase.set_UserName(String value)
at Oracle.FailSafe.Manager.Wizards.DatabaseAuthenticationPageView.Validate()
at Oracle.FailSafe.Manager.Wizards.WizardDialog.nextButton_Click(Object sender,
RoutedEventArgs e)
```

Oracle Fail Safe release 4.1.1 introduced an assertion in the client API in which all database usernames must be non-empty. The Oracle Fail Safe Manager would attempt to clear the database username when operating system authentication was chosen and that would cause an exception to be raised.

This problem has been corrected. Blank usernames are accepted again. In addition, Oracle Fail Safe Manager no longer attempts to clear the username when setting the operating system authentication.

There are a few different ways to avoid this problem:

1. Add the Oracle Fail Safe server username to the ORA_DBA group thus enabling operating system authentication for all databases accessed by the server. In this case the Authentication page is skipped
2. Use password authentication. This implies that the OS Authentication button is not checked
3. Use the Add-OracleClusterResource PowerShell cmdlet to add the database to the group

1.7.6 Starting Standby Database for Read Only With Apply Fails with ORA-1406 Error

BUG 20866996

If an Oracle Data Guard standby database is manually set to use real time apply with an open mode of `READ ONLY WITH APPLY`, when Oracle Fail Safe attempted to execute an IsAlive poll against the database, the poll would fail and the following error was posted in the Windows application event log:

```
Oracle Fail Safe resource TestDb failed to poll database.
ORA-1406: fetched column value was truncated
```

Oracle Fail Safe did not allocate enough space for the `open_mode` column which resulted in the `ORA-1406` error.

This problem has been corrected. The space allocated for fetching the open mode is increased to accommodate the `READ ONLY WITH APPLY` string. In addition, Fail Safe now properly starts and poll a standby database that is using the `READ ONLY WITH APPLY` open mode.

1.7.7 Selected Network Names not Used when Adding Database to Group

BUG 22216663

When adding a database resource to a cluster group, if the group contains more than one network name resource, Oracle Fail Safe Manager will display a selection list that allows you to select which network names to use for the group's Oracle TNS net listener address list. However, the list was not sent to the Fail Safe server which would result in the server defaulting to all the network names for the group.

This problem has been resolved. The Oracle Fail Safe Manager now sends the list of selected network names to the server.

The workaround is to manually update the group listener's description in the `listener.ora` file to only include the addresses of the desired network names. The `listener.ora` file must be updated on all cluster nodes. The changes will not take effect until the listener is restarted.

1.7.8 Oracle Fail Safe Server FsSvr.exe Fails with C0000005 Access Violation

BUGS 22537342 and 22551137

Exiting from the Oracle Fail Safe Manager or disconnecting from a server could sometimes cause the server to fail with an access violation error. The Windows event log showed an application error (`APPCRASH`) similar to the following:

```
P1: FsSvr.exe
P2: 4.1.1.2  P3: 554acfda
P4: KERNELBASE.dll
```

```
P5: 6.3.9600.17415
P6: 54505737
P7: c0000005
P8: 0000000000008b9c
P9:
P10:
```

When closing a session with the client, the server did not wait for all executing threads to terminate. All memory for the session was immediately deallocated which could result in active threads accessing memory that was reallocated to other threads.

The server has been changed to ensure that all active threads terminate before deallocating memory used by the client session.

1.7.9 Standby Database Does Not Start When it is a Container Database

BUG 23237270

If a Dataguard standby database is a multi-tenant database (CDB), it could fail to start successfully. The `FSR_TRACE_OUTPUT` file would contain the following error messages:

```
DB_RES TEST ***** OCI routine OCIStmtExecute returned error -1 - OCI_ERROR
COMMON ORA-01219: database or pluggable database not open: queries allowed on fixed
tables or views only
COMMON FscOci::StartupPdbs returning status 1219 (0x000004C3)
```

Oracle Fail Safe was attempting to execute a container database related query on a database that was not open, resulting in an `ORA-01219` error.

This error has been corrected. Now, Fail Safe will only attempt to query the standby database if it has been opened for read access.

1.7.10 Add Database to Group Fails with an FS-10712 Error When Network Resource Name is not a DNS Name

When attempting to add a database to a cluster group (role), an error was observed if the name of the cluster resource for the group's network name was not the DNS name for the network name. For example, if the DNS name for the virtual address (network name) is TestGroup, but the network name cluster resource was renamed to Network Name TestGroup, then the following error would be observed:

```
FS-10605: Oracle Net listener FslTestGroup created
0x138F: The cluster resource could not be found.
FS-10712: Failed to make resource FslTestGroup dependent on TestGroup
FS-10057: Failed to create the listener resource FslTestGroup
FS-10784: The Oracle Database resource provider failed to configure the virtual
server for resource TestDb
```

Oracle Fail Safe was incorrectly using the DNS name when attempting to create the cluster resource dependency. It should be using the actual cluster resource name.

Fail Safe now uses the resource name when creating the resource dependency.

1.7.11 Standby Database 11*g* Fails to Come Online

BUG 24488509

When adding a standby Oracle Database 11*g* to a cluster, the database fails to come online. An error similar to the following was displayed:

```
FS-10382: NODE1: Bringing resource TestStandby online
FS-10726: Resource TestStandby is in a failed state
```

If Oracle Fail Safe resource tracing `FSR_TRACE_OUTPUT` was enabled, the following error was shown in the trace output:

```
DB_RES OFS1 ***** OCI routine OCIStmtExecute returned error -1 - OCI_ERROR
COMMON ORA-02000: missing CURRENT keyword
```

This problem was introduced in patch set 3 (4.1.1.3). This patch set started a standby database which utilized Oracle Database 12*c* syntax which was not valid for Oracle Database 11*g*.

The Oracle Fail Safe server database startup is corrected to use 11*g* redo apply syntax for Oracle Database 11*g* and 12*c* syntax for Oracle Database 12*c*.

1.7.12 Add Database Fails with an FS-11373 Error

BUG 23751379

When adding a database to a cluster, a `FS-11373` error was returned when Oracle Fail Safe attempted to create the listener. For example:

```
FS-11373: Failed to create listener FslTestGroup
```

When examining the `FslTestGroup_create.log`, the following error was displayed:

```
TNS-01106: Listener using listener name Listener has already been started
```

This error occurred when another listener was listening on all IP sockets available to the host node. The default listener is typically the listener who has opened a socket for all IP addresses.

This problem is resolved. Before creating a listener, Oracle Fail Safe will stop the default listener to ensure that it is not using any IP addresses which may be needed by the new cluster group listener.

1.7.13 Standby Database has Logins Restricted After Coming Online

BUG 24700314

In Oracle Fail Safe 4.1.1, when a standby database was brought online, the database instance was set to restrict logins.

This problem is corrected. When Fail Safe starts a standby database, it allows all logins after coming online.

1.8 Known Issues

This section includes information on the following Oracle Fail Safe known issues:

1.8.1 Oracle Fail Safe Cluster Verification May Report Incorrect Patch Levels for Oracle Products

BUG 7377494

The Oracle Fail Safe cluster verification may not display the correct patch level for Oracle products. The version displayed is derived from executable images in the Oracle home for the product and might not reflect the exact patch set version stored in the inventory.

1.9 Documentation Updated for This Release

See the following documentation, which was updated for this release, for additional information:

- *Oracle Fail Safe Concepts and Administration Guide for Microsoft Windows*
- *Oracle Fail Safe Installation Guide for Microsoft Windows*
- *Oracle Fail Safe Error Messages for Microsoft Windows*
- *Oracle Fail Safe Tutorial for Microsoft Windows*

The documentation is provided in HTML and PDF online formats. Viewing the PDF files requires Adobe Acrobat Reader 3.0 or later. You can download the latest version of Adobe Acrobat Reader from the Adobe website at

http://www.adobe.com/prodindex/acrobat/readstep.html
The documentation no longer ships with the kit. The HTML and PDF formats are available on Oracle Technology Network at

http://www.oracle.com/technetwork/index.html

1.10 Additional Information About Oracle Fail Safe

See the following websites for more information about Oracle Fail Safe:

- Oracle Fail Safe on the Oracle Technology Network at

  http://www.oracle.com/technetwork/documentation/failsafe-086865.html
  Updated software compatibility information, white papers, and so on are posted on the Oracle Technology Network website.

- Oracle Support Services at

  https://support.oracle.com/

Contact your Oracle support representative for technical assistance and additional information, or visit the Oracle Support Services website to find out about other available resources.

1.11 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.