

Oracle® Fail Safe

Release Notes

Release 4.1 for Microsoft Windows

E24701-04

September 2014

This document describes the new features in this release, software errors fixed, software compatibility, hardware compatibility, and notes about installation and deinstallation.

1 How These Notes Are Organized

The remainder of these release notes are divided into the following sections:

- [Certification Information](#)
- [Installation](#)
- [New Features](#)
- [Unsupported Features](#)
- [Software Compatibility](#)
- [Disk Resources](#)
- [Problems Fixed](#)
- [Known Issues](#)
- [Documentation Updated for This Release](#)
- [Additional Information About Oracle Fail Safe](#)
- [Documentation Accessibility](#)

2 Certification Information

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

<https://support.oracle.com>

3 Installation

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

4 New Features

The following sections provide information about the new features and additions in the Oracle Fail Safe release:

- [Oracle Database 12c Support](#)
- [New Oracle Fail Safe Manager Graphical User Interface](#)
- [New Command Line Interface](#)
- [Data Guard Real-Time Apply Supported for Physical Standby Databases](#)

4.1 Oracle Database 12c Support

Oracle 12c is supported in this Oracle Fail Safe release. It also supports the new Oracle Home User feature. If a home is created with a user name, it must be a domain user account used on all nodes in the cluster. Any home which is used with a cluster database resource must be configured identically on each node in the cluster. Any home which has the same name across nodes in the cluster must use the same version, disk path, user name and password.

4.2 New Oracle Fail Safe Manager Graphical User Interface

Oracle Fail Safe introduces a new Microsoft Management Console (MMC) based utility for managing Oracle resources in Windows Failover Cluster. The new Oracle Fail Safe Manager supplements Microsoft Windows Failover Cluster Manager. Oracle Fail Safe Manager provides the basic cluster operations, such as moving a group from one node to another. It does not provide the advanced functionality, such as modifying the properties of a group. You can use Microsoft Windows Failover Cluster Manager for advanced operations which are not specific to Oracle cluster resources. Since this new GUI is an MMC snap-in, you may combine it with other MMC snap-ins to create and save custom consoles.

See Also: MMC documentation for more information about customizing the MMC interface.

4.3 New Command Line Interface

In Windows Server 2008 R2, Microsoft introduced a set of failover cluster PowerShell commands (cmdlets) as the preferred scripting tool for managing failover clusters. PowerShell is the new command and scripting language offered by Microsoft and intends to replace the old command (CMD) environment. The new failover cluster cmdlets has replaced the old command line utility, `CLUSTER.EXE`, which may not be available in the future Windows Server releases. Oracle now provides a new set of PowerShell cmdlets which has also replaced the `FSCMD.EXE` utility.

See Also: *Oracle Fail Safe Concepts and Administration Guide* to learn more about the new Oracle Fail Safe PowerShell command line interface.

4.4 Data Guard Real-Time Apply Supported for Physical Standby Databases

Oracle Fail Safe supports the Data Guard real-time apply option. It is now possible to enable or disable real-time apply using the Fail Safe Manager. Fail Safe retains the real-time apply state across database shutdown and startup.

If redo logs are not available on the physical standby database, then the real-time apply mode is ignored. The real-time apply option is not presented for logical standby databases by the Fail Safe Manager. Databases real-time apply starts if redo logs are enabled for logical standby.

Note: Data Guard Broker is not referenced or maintained by Fail Safe

5 Unsupported Features

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

- [Application Services Not Supported](#)
- [32-Bit Server Platforms Not Supported](#)
- [Multitenant Container Databases Not Supported](#)

5.1 Application Services Not Supported

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

5.2 32-Bit Server Platforms Not Supported

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

5.3 Multitenant Container Databases Not Supported

Oracle Fail Safe 4.1 is not supported in a multitenant container database environment. Oracle Fail Safe Release 4.1.1, targeted for the first half of 2015, will support a multitenant container database environment.

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.

Oracle Fail Safe Manager is compatible with the following operating systems:

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2012
- Windows 7
- Windows 8

Note: Oracle Fail Safe Manager has compatibility issues with Microsoft Windows Server 2012 and Windows 8. Refer [Section 9.2, "Oracle Fail Safe Manager Display Issues with Windows"](#) for more information.

Oracle Fail Safe Manager is also compatible with Oracle Fail Safe Server version 3.4.2.4 and later patch sets.

Oracle Fail Safe Server is compatible with the software listed in the following table:

Software	Release or Version
Oracle Database (Standard and Enterprise editions)	Oracle Database 11g Release 2 (11.2)
	Oracle Database 12c Release 1 (12.1)
Oracle Management Agent	Release 11.2
	(A Management Agent release for Microsoft Windows only)
Microsoft Windows Platforms	Microsoft Windows Server 2008
	Microsoft Windows Server 2008 R2
	Microsoft Windows Server 2012

Note:

- Oracle Fail Safe does not support Oracle Automatic Storage Management
 - Oracle Fail Safe Server does not support 32-bit operating systems
 - Oracle Fail Safe Server is only supported on Windows Server systems, it is not supported on non-server systems such as Windows 7 and Windows 8
-
-

7 Disk Resources

Oracle Fail Safe allows the use of EMC SRDF/CE disks, formerly known as EMC GeoSpan. However, if you attempt to add a resource to a group and an EMC SRDF/CE disk used by the resource that is not present in that group, then Oracle Fail Safe returns the error `FS-10203`, and rolls back the operation.

If this occurs, add the resource to the group that contains the EMC SRDF/CE disk that the resource requires.

8 Problems Fixed

This section includes information on Oracle Fail Safe problems fixed since release 3.4.2.0.

8.1 Security Setup Tool Shows Incorrect Password

Bug 9764287

When using Oracle Services for the Microsoft Windows Failover Clusters Security Setup tool, if an incorrect password is entered three times in a row, further attempts to enter the password fails, even if the password is correct. To successfully enter the correct password, you must exit from the tool and login again.

The tool to set the Oracle Fail Safe server credentials is rewritten and this problem no longer occurs.

8.2 Security Setup Tool Stops Responding if FSS_TRACE_OUTPUT is Invalid

Bug 8368535

If Oracle Fail Safe tracing is enabled, and the output file represented by the FSS_TRACE_OUTPUT registry value is not a valid file specification, Oracle Services for Microsoft Windows Failover Clusters Security Setup tool stops responding.

The tool to set the Oracle Fail Safe server credentials is rewritten and this problem no longer occurs.

8.3 Space in the Parameter File Path Shows an FS-10616 Error When Adding Database to a Group

BUG 9670567

Databases which have a space character in the file specification for the parameter file cannot be added to a cluster group. For example, if there is a space character between param and file in the file specification H:\OFS2\param file\INITOFS2.ora, the command fails with the following error:

```
** ERROR : FS-10616: Failed to open Windows service OracleServiceORCL  
** ERROR : 0x424: The specified service does not exist as an installed service
```

When Oracle Fail Safe creates a database instance, it uses the lsnrctl utility to create the Windows service. One of the parameters which moves to the utility is the file specification for the database parameter file. If Fail Safe does not quote the file specification accurately and there is a space character in the path name, then the lsnrctl utility incorrectly parses the parameter file name.

Oracle Fail Safe now properly quotes the parameter file name when passing it to the lsnrctl utility.

8.4 Failover Policy Changes Not Applied Correctly

BUG 9591157

When the failover policies for an Oracle Enterprise Manager agent cluster resource changes using the Oracle Fail Safe Manager, the changes are not applied to the resource.

This problem is resolved in the new Oracle Fail Safe Manager graphical user interface. Cluster resource property changes are now applied correctly, regardless of the resource type.

8.5 Database Stops Responding or Shows an Error ORA-12631

BUG 9560606

If the Windows service for a database instance or a database listener with the option Log On As changes from the default local system account to a specific user account, database fails or shows the following error:

```
ORA-12631: Username retrieval failed
```

This problem occurs as Oracle Fail Safe does not provide a fully qualified account name that includes the authentication domain. The connect string must contain a user name instead of a domain/user name.

This problem is resolved and the error no longer occurs.

8.6 WMI Applications Fail to Access Oracle Groups

BUG 9527244

Applications which use the Windows Management Instrumentation (WMI) provider, such as the EMC Cluster Enabler, show errors when loading resources from cluster groups that contain Oracle databases. For example, the EMC Cluster Enabler reports the following error when it attempts to access a cluster group containing an Oracle database:

```
Cluster Enabler 3.X: CeCluster BuildCeDevices failed. An unexpected error occurred when building devices for CE
```

The CE Event trace log contains output similar to the following when the log level is set to 5:

```
ERROR N/A NODE10 GUI_BL CeCluster::BuildCeDevices An unexpected error occurred when building devices for CE. Exception: Message: Invalid operation N/A
VERBOSE N/A NODE10 GUI_BL CeCluster::PrintCeDeviceList Print out CeDevice list:
N/A
ERROR N/A NODE10 GUI_BL CeCluster::CeCluster BuildCeDevices failed. An unexpected error occurred when building devices for CE. N/A
VERBOSE N/A NODE10 GUI_BL CeCluster::BuildCeDevices Exiting. N/A
VERBOSE N/A NODE10 GUI_BL CeCluster::PrintCeDeviceList CeDevice #[1]: Unique id [2757804048] Mirror pair [SYMMETRIX+000290103239 03FB SYMMETRIX+000290103279 03FB]
N/A
VERBOSE N/A NODE10 GUI_BL CeRoot::AddCeCluster Exiting. N/A
ERROR N/A NODE10 GUI CE_RootScopeNode::ManageCluster An error occurred when gathering information for CE Cluster on server [.]. BuildCeDevices failed. An unexpected error occurred when building devices for CE. N/A
```

Oracle Fail Safe always uses a cluster resource private property named Instance to record the instance name of an Oracle database in a cluster. Instance is a reserved word in the WMI architecture, so when the Windows Failover Cluster WMI provider attempts to present the database private properties to a WMI data consumer, it shows an error when it encounters the instance property.

This problem is resolved. Oracle Fail Safe now uses the name DBInstance to represent the database instance resource private property. Existing cluster databases continue to use the instance private property name until the database is removed from the cluster group or a Fail Safe Verify Cluster command is issued. If all nodes in a cluster are upgraded to the new Fail Safe Server, when the Verify Cluster command is issued, all Oracle databases have their instance private property renamed to DBInstance. Also, if a database is removed from a group and then added back, Fail Safe server uses the name DBInstance for the instance private property. If it becomes necessary to downgrade to an older release of Oracle Fail Safe, then all databases must be removed from the cluster groups prior to downgrading as older versions of Fail Safe will not recognize the DBInstance property name.

8.7 0xEA: More Data is Available Error from Various Operations

BUG 9843142

Various Fail Safe operations, such as Verify Cluster, fails with an output similar to the following error:

```
** ERROR : 0xEA: More data is available
```

This error occurs when Oracle Fail Safe searches for the network IP addresses for a cluster node. In some instances, Oracle Fail Safe does not allocate enough buffer space for the cluster node information returned.

This problem is corrected. Oracle Fail Safe now handles this error correctly when insufficient buffer space is allocated.

8.8 Resource Monitor Fails with an Exception Code Error

BUG 9855380

When there are multiple database resources monitored by Oracle Fail Safe, the cluster resource monitor may fail with access violations such as exception code 0xc0000005 or other similar errors. These errors vary for the Windows and Fail Safe versions. In Fail Safe release 3.4.2 running on Windows Server 2008, entries in the Windows application log such as Application Error {100} N/A and Faulting application rhs.exe appear incorrectly. If Oracle Fail Safe version is 3.4.1, then you may see an application log entry similar to the following:

```
Oracle Fail Safe caught an unexpected error 5 (0xC0000005) in module odbc.c at line
```

```
Oracle Fail Safe caught an unexpected error 5 (0xC0000005) in module ..\FscLib\FsDdbsUpi.c at line
```

On Windows Server 2003 systems, the incorrect application is ResrcMon.exe.

This problem is caused by a Oracle Fail Safe component which gets information from Oracle installation homes which is not safe and may access free memory or memory allocated to other uses.

This problem is corrected. Oracle Fail Safe now uses safe methods to get information from Oracle homes.

8.9 Adding Generic Resource to a Group Fails with an Error

BUG 9918518

When adding a generic resource to a group, if the executable for the resource is on a shared disk, the operation fails with error output similar to the following:

```
FS-10381: CLUNODE1 : Creating the resource information for resource My Generic Service
0x138F: The cluster resource could not be found
FS-10006: Unable to open the resource S:\App\Bin\MyGenServ.exe
FS-10717: Failed to read the common properties for resource S:\App\Bin\MyGenServ.exe in the cluster
FS-10778: The Generic Service resource provider failed to configure the cluster resource My Generic Service
FS-10890: Oracle Services for MSCS failed during the add operation
```

When a generic resource is added to a group, Oracle Fail Safe checks if the resource depends on a shared disk. If a shared disk is needed to run the resource, then that disk is added as a dependency for the generic service resource. However, Fail Safe uses the actual image path rather than the disk resource name when it attempts to create the dependency. That results in an error since the path string is not a valid resource name.

This problem is corrected. Oracle Fail Safe uses the actual resource name for the disk rather than the image path when creating the dependency.

8.10 FS-11001 Errors When Executing Oracle Fail Safe Commands

BUGs 9796843, 9967279

When executing Oracle Fail Safe commands which require loading node configuration information, you may get an error similar to the following:

```
FS-10660: Node2 : Gathering cluster information
FS-11001: Message 11001 not found; product=OracleFailSafe; facility=FS
```

This error occurs when there is an IP address assigned to a cluster group which does not have an associated network name in the group. As a result, several problems are triggered. When there is no network name for the IP address, Oracle Fail Safe uses the IP address as the network name. It attempts to find all the IP addresses associated with the network name, treating the IP address string as a fully qualified domain name string. Oracle Fail Safe isolates a nodename from a fully qualified domain name by searching the nodename string for a period and using the string to the left of the period as a nodename. Then, Oracle Fail Safe uses that string to search for IP addresses. When this strategy is applied to an IP address string, the result is a nodename that is a numeric string.

For example, for the IP address 192.168.0.2, Oracle Fail Safe isolates the 192 and then attempts to search for the IP address for a node named 192. Since this nodename does not exist, Windows returns a No such host is known error, which has an error code of 11001. Oracle Fail Safe incorrectly interprets the error as an Oracle Fail Safe error and attempts to locate the message string in the Oracle Fail Safe messages file. Since the error is not a Fail Safe error code, it displays an error Message 11001 not found.

This problem can be avoided by ensuring that all IP addresses in a cluster group have a corresponding network name that resolves to that IP address.

Oracle Fail Safe no longer attempts to interpret an IP address string as a fully qualified domain name.

8.11 FS-10066: Failed to Start Windows Service Error When Adding a Database Resource

BUG 10034845

When adding a database to a cluster group, the operation may fail with an error similar to the following:

```
FS-10066: Failed to start Windows service
OracleOraDb11g_home1TNSListenerFslTestDB for the Oracle Net listener
FS-10065: Error trying to configure the Oracle Net listener
```

When configuring a database network listener, Oracle Fail Safe spawns processes to execute the appropriate listener commands required for setting up the listener. Fail Safe attempts to direct the output from those commands to the oracle_home\NETWORK\log directory and if that directory cannot be found, then it attempts to send the output to the nul device. This problem occurs when the ORACLE_HOME directory for the database home contains the string \admin. For example, if the ORACLE_HOME is C:\app\administrator\product\11.2.0\dbhome_1, then the error occurs. Oracle Fail Safe is using inadequate directory parsing when attempting to locate the \NETWORK\log directory. In addition, if the directory cannot be found, the spawned process fails when attempting to write to the nul device setup by Fail Safe.

Oracle Fail Safe is corrected to properly locate the `oracle_home\NETWORK\log` directory. If the desired output directory cannot be located, the spawned process no longer encounters errors trying to write to the `stdout` file.

The error can be avoided by installing Oracle database in a directory that does not contain `\admin`.

8.12 Database Fails to Restart

BUG 10160858

When a database is forced to go offline due to a failure in the cluster group, it does not restart until the group fails in another node. If Oracle Fail Safe resource monitor tracing `FSR_TRACE_OUTPUT` is enabled, text similar to the following may be present in the trace file:

```
<DB_RES> Oracle Fail Safe resource SDB_112 is being forced offline
<DB_RES> Oracle Fail Safe resource SDB_112 successfully forced offline
<DB_RES> Oracle Fail Safe resource SDB_112 is starting
<DB_RES> SDB_112 starting

<DB_RES> Event start
FscOci::Connect called when connection active
<DB_RES> Event end

<COMMON> FS-10999: An internal programming error has occurred
```

When a database is forced to go offline, the resource monitor does not properly reset its OCI context, resulting in an error when it attempts to reconnect to the database.

This problem is corrected and the Oracle Fail Safe resource monitor now resets the OCI context when a database is forced to go offline.

8.13 FS-10751 and FS-10755 Errors after Upgrading From Oracle Fail Safe Release 3.3.4

BUGs 8683154 and 8794424

If a system is upgraded from Oracle Fail Safe release 3.3.4 without deinstalling the old version of Fail Safe, commands such as `Verify Cluster` fails with errors similar to the following:

```
0x80080005: Server execution failed
FS-10751: Node NODE1 failed to create a class factory on remote node NODE2
FS-10755: Error creating the OracleFsWorker COM object
```

This error is caused by an invalid Access Control Entry (ACE) in the Access Control List (ACL) for the Oracle Fail Safe COM class. This problem only occurs when an old ACL is updated to the newer format. When a new installation is done instead of upgrading an existing installation, the error does not happen.

Microsoft Windows Server 2003 SP1 introduced a new COM ACE format that requires that all ACLs completely conform to the new format or not use the new format. Fail Safe releases after 3.3.4 use the new format for creating new ACLs, but before this patch set, Fail Safe did not attempt to convert existing ACEs to the new format. When updating existing ACLs, the older ACEs may sometimes be combined with new format ACEs, which causes any access to the Oracle Fail Safe COM class to fail.

For more information, refer the Microsoft Development Network (MSDN) article at:

<http://msdn2.microsoft.com/en-us/library/ms693364.aspx>

This problem is corrected. If Oracle Fail Safe encounters a COM ACL that contains the old format ACE, it converts the old ACE to the new format.

8.14 FsSvr.exe Error During Oracle Fail Safe Installation

BUGs 10192722 and 11829037

When installing Oracle Fail Safe or when running the Oracle Services for Microsoft Windows Failover Clusters Security Setup utility, a message box appears with the text Oracle Services for MSCS has stopped working. The Windows application event log contains an entry similar to the following:

```
Error 2011/02/21 15:34:44 Application Error 1000 (100)
Faulting application fssvr.exe, version 3.4.2.0, timestamp 0x4b26a129,
faulting module ntdll.dll, version 6.0.6002.18005, timestamp 0x49e042a129,
exception code 0xc0000374 fault address 0x00000000000aef37, ...
```

The problem occurs when the Oracle Fail Safe server process `FsSvr.exe` scans the cluster resources searching for the cluster network name. The error happens when a shorter network name string encounters before locating the cluster network name. The server process initially allocates a buffer for the shorter network name string and then attempts to use the same buffer for reading the longer network name. When the longer network name is read, memory gets corrupted resulting in the `0xc0000374` error, or a `STATUS_HEAP_CORRUPTION` error.

This problem is corrected.

8.15 Cluster Resource Monitor Fails with an Access Violation

BUG 12368992

When an Oracle Database resource is terminated, the cluster resource monitor may fail with an access violation exception code `0xc0000005`. This may fail if the termination occurs when the resource monitor executes an `IsAlive` poll. Examining the process dump shows a stack trace similar to the following:

```
FscLib!FscOci::FetchDbRoleAndOpenMode+0x5ab
msvcr80!_CallSettingFrame+0x20
msvcr80!__CxxCallCatchBlock+0xfe
ntdll!RcFrameConsolidation+0x3
FscLib!FscOci::FetchDbRoleAndOpenMode+0x39d
FscLib!FscOci::IsAlive+0xb0
FsResOdb!Startup+0x4864
```

This problem occurs because Oracle Fail Safe does not properly handle multi-threaded requests in the resource monitor. Concurrent `IsAlive` and `Terminate` requests do not guard against the possibility of other threads executing the same database access routines at the same time. When you receive the `Terminate` request, the Fail Safe resource monitor clears the database context without checking if any other threads are using the database context. That may result in failures when OCI routines are accessed by other threads at the same time.

This problem is corrected. A `Terminate` request ends the `IsAlive` thread before clearing the database context.

8.16 Database Resource Fails to Start

BUG 12434216

If a cluster has Oracle Database 10g Release 2 installed without any newer database versions such as Oracle Database 11g, and there is no database home \bin directories in the system path environment variable, the database resource fails to start. The Windows application event log contains an entry similar to the following error:

```
Oracle Fail Safe resource SDB_102 failed to start
FS-10999: An internal programming error has occurred
```

If you attempt to add a database to a group, it results in a progress window output similar to the following text:

```
Resource SDB_102 is in a failed state
Failed to bring the cluster resource SDB_102 online. Check the Windows event log
for messages
The Oracle Database resource provider failed to bring resource SDB_102 online
Oracle Services for MSCS failed during the add operation
```

If the Oracle Fail Safe cluster resource monitor tracing facility (FSR_TRACE_OUTPUT) is enabled, the trace file will contain the following text:

```
<DB_RES> SDB_102 ***** OCI routine OCIEnvNlsCreate returned error -1
<COMMON> FS-10999: An internal programming error has occurred
```

This problem occurs when the Oracle Fail Safe resource monitor fails to initialize the Oracle Call Interface (OCI). The OCI interface does not initialize because it fails to locate the necessary Oracle Database DLL files. It only happens when using Oracle Database versions older than Oracle Database 11g. In the previous versions of Oracle Database, OCI attempted to find the ORACLE_HOME environment variable and use that home to find the Oracle database DLL files. However, the resource monitor may not have ORACLE_HOME declared, so initialization fails. In Oracle Database 11g, the OCIEnvNlsCreate function changes to use the directory where the OCI.DLL file resides to locate the Oracle Database DLL files.

The workaround is to include an Oracle Database home \bin directory in the system path environment variable, or install a release of Oracle Database newer than 10g Release 2.

This problem is corrected. Oracle Fail Safe now sets the default DLL directory to the Oracle Database home before calling OCIEnvNlsCreate. This ensures that the files necessary for OCI can be located.

8.17 Resource Monitor Fails With Access Violation

BUG 12597932

If a database instance fails, for example, by stopping the Windows service, the cluster resource monitor may report an access violation error and exit. When the resource monitor fails, all the resources managed by the resource monitor move to another node.

This problem is caused by a function in the Oracle database resource monitor. The terminate function starts a thread to asynchronously disconnect and cleanup the old database context. Then, the online function tries to create a new database context. If the online function runs before the disconnect function completes, the disconnect function resets the database context created by the online function.

This problem is corrected. The terminate function now waits for all the disconnected activities to complete before allowing the online function to proceed.

8.18 Enterprise Manager Agent Resource Not Created

BUG 11718828

When Oracle Fail Safe creates an Oracle Enterprise Manager agent as a cluster resource, it does not create a dependency on the network name that the agent needs for network connections. This causes errors if the network name is not online when attempting to control the agent using the `emctl` utility.

This problem is resolved. Oracle Fail Safe now creates a dependency relationship, where the cluster group network name must be online before the agent starts, and the agent must stop before stopping the network name.

8.19 Listener Name Incorrectly Contains a Hyphen

BUG 8416715

When Oracle Fail Safe adds a database to a cluster group, it creates a database network listener if it was not previously created in the group. The name for the listener is derived from the group name. Previously, if a group name contained a hyphen, then Fail Safe created a listener with the hyphen in the listener name. However, listener names must only contain alphanumeric characters or an underscore, hyphens are not allowed.

This problem is resolved. Oracle Fail Safe now creates a new listener it converts hyphens in the group name to underscores.

8.20 Server Fails with Access Violation When Adding Database to a Group

BUG 12543894

If the default listener for a database home has an address that contains a port number but no host name, Oracle Fail Safe server fails with an access violation error C0000005 when searching for the default listener in the `listener.ora` file. Oracle Fail Safe server looks for the default listener when executing database actions such as Verify Database or Add Resource. The following `listener.ora` file entry may cause server failure:

```
LISTENER =
  (ADDRESS_LIST=
    (ADDRESS=
      (PROTOCOL=TCP)
      (Port=1521)
    )
  )
```

When the server fails, if a process dump is created, it has a stack trace with the following call frames:

```
FscLib!FspNlMatchHost+0x70
FscLib!FspNlAddrListHasOneHost+0x68
FscLib!FspNlFindLisByLisInfo+0x19f
FscLib!FscSqlnetUtility::GetDefaultListener+0xa16
```

This problem occurs because the Fail Safe server assumes that every listener address has a name associated with it. The problem does not occur if there is a `Host=` tag is included in the address declaration.

This problem is resolved. When parsing the listener.ora file, Oracle Fail Safe server ignores address entries that do not contain a host name.

8.21 FS-10242 Error When Default Listener Address Host is Not Numeric

BUG 12869279

When adding a database to a group or verifying a standalone database, if the default listener has an ADDRESS entry with a HOST that is not a numeric IP address, you may get the following error:

```
FS-10380: NODE1 : Configuring virtual server information for resource OFS1
FS-10230: The Oracle Net listener LISTENER uses a host name in the host address
parameter. It must be converted to use an IP address
FS-10231: The listener is currently running
FS-10233: Do you want to stop the listener, convert the host name to an IP
address, and then start the listener again?
  Yes
FS-11004: Message 11004 not found; product=OracleFailSafe; facility=FS
FS-10223: Cannot resolve network name ?? to an IP address on the system for
validation due to a secondary error
FS-10242: Failed to get the IP address of host NODE1
FS-10240: Failed to reconfigure Oracle Net listener LISTENER to use an IP address
FS-10784: The Oracle Database resource provider failed to configure the virtual
server for resource OFS1
FS-10890: Oracle Services for MSCS failed during the add operation
```

It is also possible to get an FS-10222 error instead of the FS-11004 and FS-10223 errors.

```
FS-10222: Cannot resolve network name ?? to an IP address on node NODE1
```

This problem may occur when a name string is used in the listener.ora file for the HOST parameter. For example:

```
LISTENER =
  (ADDRESS_LIST=
    (ADDRESS=
      (PROTOCOL=TCP)
      (Host=NODE1)
      (Port=1521)
      (ADDRESS=
        (PROTOCOL=IPC)
        (KEY=EXTPROC0)
      )
    )
  )
```

The workaround is to replace the Host=NODE1 text string with a numeric IP address. For example, Host=192.168.0.2.

Another workaround is to click **No** when you see the query FS-10233: Do you want to stop the listener, convert the host name to an IP address, and then start the listener again?

The following message can be safely ignored:

```
FS-10230: The Oracle Net listener LISTENER uses a host name in the host
address parameter. It must be converted to use an IP address.
```

It is not mandatory to convert the host name to an IP address.

The cause of the problem is an incorrect parameter which passes to an Oracle Fail Safe networking subroutine.

This problem is fixed. The correct parameter now passes to the networking subroutine.

8.22 FS-10066 and FS-10065 Errors When Removing Database From a Group

BUG 13058347

When removing a database from a group, if there is no default listener declared in the `listener.ora` file, then no default listener is created and the database is not assigned to any listener. If Oracle Fail Safe patch set 3.4.2.3 is installed, error similar to the following is displayed:

```
WARNING : 0x426 : Failed to start the service
WARNING : FS-10066: Failed to start Windows service
OracleOraDb11g_home1TNSListenerFslgroupname for the Oracle Net listener
WARNING : FS-10065: Error trying to configure the Oracle Net listener
```

When there is no default listener declared, Oracle Fail Safe assigns the database to the listener that was deleted when removing the database from the group. Prior to the patch set 3.4.2.3, this error was ignored.

This problem is corrected. If no default listener is declared in the `listener.ora` file, it is created and the database is assigned to that listener.

8.23 ORA-01031 Error When Changing Database System Password

BUG 13691346

Oracle Fail Safe Manager utility can change the system user password of a database in the Authentication Properties page. In Oracle Fail Safe release 3.4.2, this functionality does not work correctly. If you attempt to change the system password, it shows the following error:

```
FS-10890: Oracle Services for MSCS failed during the put_data operation
FS-10757: A COM error was returned when trying to send a work item to the worker
FS-10990: The error 0x80040407 was reported as a system error, but the error
message cannot be found
ORA-01031: insufficient privileges
```

When connecting to the database in Oracle Fail Safe release 3.4.2, the server uses the new database password instead of the current database, which results in an ORA-01031 error.

The Oracle Fail Safe server is corrected. The change password function now uses the current password when connecting to a database.

8.24 ORA-12560 Error When Changing the Open Mode Function of a Database

BUG 13893012

When a database is setup as an Oracle Data Guard Standby database, you can change the open mode function to read only or mounted using the Oracle Fail Safe Manager utility. When you attempt to change the open mode function of a database in Oracle Fail Safe release 3.4.2, it shows the following error:

FS-10890: Oracle Services for MSCS failed during the changeDBOpenMode operation
ORA-12560: TNS:protocol adapter error

When connecting to the database in Oracle Fail Safe release 3.4.2, the server does not use the correct database service ID SID, resulting in an ORA-12560 error.

The Oracle Fail Safe server is corrected. The change open mode function now uses the correct SID when connecting to a database.

9 Known Issues

This section includes information on Oracle Fail Safe known issues.

9.1 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.

9.2 Oracle Fail Safe Manager Display Issues with Windows

On Windows 8 and Microsoft Windows Server 2012 systems, Oracle Fail Safe Manager may not display dialog boxes correctly. Windows may not display the graphical user interface (GUI) elements with the correct layering or z-order.

For example, if you click a drop-down list in a dialog box, the dialog box will drop behind its parent window, leaving the drop-down list displayed over the parent window instead of the dialog box that it belongs to. Similarly, in a dialog box with a tooltip, if you move your cursor over the window, the tooltip is displayed but the dialog box will drop behind its parent window.

This issue exists in previous versions of Windows, but with the upgrade of Microsoft Management Console (MMC) to .NET 4.0 this issue is now seen in MMC applications that use Microsoft Windows Presentation Foundation (WPF) to create forms. The new Oracle Fail Safe Manager is MMC based and uses the WPF in most windows and dialog boxes. Thus, the new Fail Safe Manager is likely to encounter the z-order issues. Oracle is working with Microsoft for a solution to this issue.

To avoid these issues, install Oracle Fail Safe Manager on a Microsoft Windows Server 2008 or a Microsoft Windows 7 system and remotely manage clusters from that system.

10 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 Web site 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 the Oracle Technology Network.

11 Additional Information About Oracle Fail Safe

Refer to the following Web sites for more information about Oracle Fail Safe:

- Oracle Fail Safe on the Oracle Technology Network

<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 Web site.

- Oracle Enterprise Manager on the Oracle Technology Network

<http://www.oracle.com/technetwork/indexes/documentation/index.html#em>

- Oracle Support Services

<https://support.oracle.com/>

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

12 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 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.

Oracle Fail Safe Variables File, Release 4.1 for Microsoft Windows
E24701-04

Copyright © 2012, 2014, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in

dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

