Oracle® Fail Safe
Release Notes
Release 3.1.2 for Windows NT and Windows 2000
January 2001

How These Notes Are Organized
These release notes are divided into the following sections:

- New Features for This Release
- Software Compatibility
- Installation and Deinstallation
- Oracle Fail Safe Server
- Oracle Fail Safe Manager
- Oracle Databases
- Oracle Reports
- Oracle Forms Load Balancer Server
- Oracle Application Server
- Oracle MTS Service
- Disk Resources
- Clients and Applications
- Oracle Enterprise Manager Integration
- Documentation Updated for This Release
- Documentation Errors
- Obsolete Features
- Software Errors Fixed

Oracle is a registered trademark, and JInitiator, Net8, Oracle8, Oracle8i, and SQL*Net are trademarks or registered trademarks of Oracle Corporation. Other names may be trademarks of their respective owners.
New Features for This Release

Oracle Fail Safe provides high availability on Microsoft clusters for a complete Internet business solution. This release of Oracle Fail Safe provides the following new features:

- Support for configuring an Oracle Service for Microsoft Transaction Server (MTS) for high availability. (In the documentation, Oracle Service for MTS is referred to as Oracle MTS Service.)
- Support for error handling scripts for errors that occur when Oracle Fail Safe attempts to bring a highly available database online.
- Support for Windows operating system (OS) authentication for database authentication.
- Support for Oracle iAS 1.0.1, with the exception of Oracle 8i Cache

Software Compatibility

This section describes the software with which Oracle Fail Safe is compatible when installed on Windows NT or Windows 2000, respectively.

Oracle Fail Safe Compatibility When Installed on Windows NT

This release of Oracle Fail Safe is compatible with the software shown in the following table when Oracle Fail Safe Server is installed on Microsoft Windows NT Enterprise Edition 4.0 (Service Pack 3, 4, 5, or 6a), and Oracle Fail Safe Manager is installed on one of the following:

- Microsoft Windows NT 4.0 (Service Pack 3, 4, 5, or 6a)
- Windows 95 OEM SR2
- Windows 98
- Windows 2000

<table>
<thead>
<tr>
<th>Software</th>
<th>Release or Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Cluster Server (MSCS)</td>
<td>Version 1.0</td>
</tr>
<tr>
<td></td>
<td>Build 224</td>
</tr>
<tr>
<td>Oracle database server</td>
<td>Oracle 7.3.4</td>
</tr>
<tr>
<td></td>
<td>Oracle 8.0.6</td>
</tr>
<tr>
<td></td>
<td>Oracle 8.1.5</td>
</tr>
<tr>
<td></td>
<td>Oracle 8.1.6</td>
</tr>
<tr>
<td></td>
<td>Oracle 8.1.7</td>
</tr>
</tbody>
</table>
Oracle Fail Safe Compatibility When Installed on Windows 2000

This release of Oracle Fail Safe is compatible with the software shown in the following table when Oracle Fail Safe Server is installed on Microsoft Windows 2000 Advanced Server or Datacenter Server, and Oracle Fail Safe Manager is installed on one of the following:

- Microsoft Windows NT 4.0 (Service Pack 3, 4, 5, or 6)
- Windows 95 OEM SR2
- Windows 98
- Windows 2000

### Software Compatibility Table

<table>
<thead>
<tr>
<th>Software</th>
<th>Release or Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Service for MTS(^1)</td>
<td>Oracle 8.1.6</td>
</tr>
<tr>
<td></td>
<td>Oracle 8.1.7</td>
</tr>
<tr>
<td>Oracle Enterprise Manager</td>
<td>Release 2.0.4</td>
</tr>
<tr>
<td></td>
<td>Release 2.1</td>
</tr>
<tr>
<td></td>
<td>Release 2.2</td>
</tr>
<tr>
<td>Oracle Forms Load Balancer Server</td>
<td>Release 6.0.1.0 and later</td>
</tr>
<tr>
<td>Oracle Forms Server 6(^2)</td>
<td>Release 6.0.8.7.3 and later</td>
</tr>
<tr>
<td>Oracle Reports Server 6(^i)</td>
<td>Release 6.0.8.8.3 and later</td>
</tr>
<tr>
<td>Oracle Application Server</td>
<td>Release 4.0.8.1</td>
</tr>
<tr>
<td></td>
<td>Release 4.0.8.2</td>
</tr>
<tr>
<td>Oracle Applications</td>
<td>Release 11.5.1</td>
</tr>
<tr>
<td>Oracle HTTP Server</td>
<td>Release 1.3.9</td>
</tr>
<tr>
<td></td>
<td>Release 1.3.12</td>
</tr>
<tr>
<td>Oracle WebDB</td>
<td>Release 2.1</td>
</tr>
<tr>
<td></td>
<td>Release 2.2</td>
</tr>
<tr>
<td></td>
<td>Release 2.5</td>
</tr>
<tr>
<td>Oracle Intelligent Agent</td>
<td>Release 8.1.7</td>
</tr>
<tr>
<td>Oracle iAS (except Oracle 8i Cache)</td>
<td>1.0.1</td>
</tr>
</tbody>
</table>

\(^1\) Oracle Service for MTS is installed with the Oracle database server.

\(^2\) Oracle Corporation recommends that you use JInitiator release 1.1.7.15.1 or later to display Oracle Forms on the Web.

---

Oracle Fail Safe Compatibility When Installed on Windows 2000

This release of Oracle Fail Safe is compatible with the software shown in the following table when Oracle Fail Safe Server is installed on Microsoft Windows 2000 Advanced Server or Datacenter Server, and Oracle Fail Safe Manager is installed on one of the following:

- Microsoft Windows NT 4.0 (Service Pack 3, 4, 5, or 6)
- Windows 95 OEM SR2
- Windows 98
- Windows 2000

### Microsoft Cluster Server (MSCS) Compatibility Table

<table>
<thead>
<tr>
<th>Software</th>
<th>Release or Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Cluster Server (MSCS)</td>
<td>Version 5.0</td>
</tr>
</tbody>
</table>
Installation and Deinstallation

This section includes topics about Oracle Fail Safe installations.

For complete installation and deinstallation instructions, see the *Oracle Fail Safe Installation Guide*.

**Workaround for Failed Deinstallation of Oracle Fail Safe 3.0.3 and 3.0.4**

If you are deinstalling or upgrading from Oracle Fail Safe 3.0.3 or 3.0.4 and the installer exits before the installation or deinstallation is completed, perform the following actions:

1. Stop Oracle Fail Safe Server with the Cluster Administrator. Make sure that Oracle Fail Safe Server is stopped on all cluster nodes.

2. Remove the Oracle Fail Safe component files from the Oracle installer directory (for example, C:\Program Files\Oracle\Inventory\Components). Remove only the files that begin with oracle.failsafe.

**Reboot Twice After Upgrading from Oracle Fail Safe 2.1.3 to Oracle Fail Safe 3.1.2**

After the installation is completed, the Oracle Fail Safe 3.1.2 installer will instruct you to reboot the system. This reboot will update the system path to include the Oracle Fail Safe 3.1.2 directory.

If you are upgrading from Oracle Fail Safe release 2.1.3, then after the first reboot, run Verify Cluster in Oracle Fail Safe Manager to update the Oracle Fail Safe database resource DLL. Then reboot each cluster node a second time, so the cluster services can pick up the new resource DLL.

**MSCS Cluster Administrator Displays Problems with Fail-Safe Resource Types**

Sometimes, after completing an Oracle Fail Safe installation, you see problems with the fail-safe resource types (databases, Oracle Application Server, and so on) in MSCS Cluster Administrator. MSCS Cluster
Administrator denotes the problem by displaying a red Oslash symbol (Ø) over the resource type name.

If this occurs, do the following:

1. If you forgot to reboot the cluster nodes after installing Oracle Fail Safe, do so now.

2. Make sure that the PATH environment variable includes the Oracle Fail Safe Server path. (In the Command Prompt window, enter PATH. The Oracle Fail Safe Server path (<Oracle_Home>/fs/fssvr/bin) should be included. If it is not included, add it, and then reboot the nodes on which the Oracle Fail Safe Server path is missing.

3. Make sure that the problem resource DLL or DLLs for the resource types are installed in <Oracle_Home>/fs/fssvr/bin. The resource DLLs are:
   - fsresodbs.dll (for the Oracle database component)
   - fsresoas.dll (for the Oracle Application Server component)
   If the resource DLLs are not there, reinstall Oracle Fail Safe (and select the components that you want), then reboot all cluster nodes.

4. Use Oracle Fail Safe Manager to verify the cluster (on the Troubleshooting menu, click Verify Cluster), then reboot each cluster node, one at a time. The Verify Cluster command automatically verifies registration of Oracle resource DLLs (as described in the next section). You may not need to reboot all cluster nodes. After you reboot one node, check MSCS Cluster Administrator to see if the Oslash symbol has been removed from the resource type name. If the Oslash symbol is gone, you do not need to reboot all cluster nodes.

**Verify Cluster Command Automatically Verifies Registration of Oracle Resource DLLs**

Prior to release 3.0.3, the Oracle Fail Safe installation procedure would automatically register and unregister the Oracle resource DLL files with the MSCS software. However, if there were problems with the registration, you would have to manually reregister the resource DLLs. Beginning with Oracle Fail Safe release 3.0.3, you can run the Verify Cluster operation to automatically reregister resource DLLs. Thus, if you receive an error message saying that the Oracle resource DLL files are not registered properly, run the Verify Cluster command to reregister them.

Appendix C in the *Oracle Fail Safe Installation Guide* describes the resource DLLs. (This appendix also describes the manual method for registering or unregistering resource DLLs, but the preferred method is to use Verify Cluster.)
Silent Installation Is Case-Sensitive

The Oracle Fail Safe silent installation is case-sensitive. You must enter all command-line syntax exactly as shown in the *Oracle Fail Safe Installation Guide* (for example, the `-responseFile` parameter must be entered using all lowercase characters, except for the F, as shown). You must enter the file specification using the case shown in Windows Explorer (for example C:\Ofs\Silent_Install\OfsProducts.rsp).

Oracle Fail Safe Client and Server Releases Must Match

If you are performing a rolling upgrade of the Oracle Fail Safe software, you must upgrade the Oracle Fail Safe Server and Oracle Fail Safe Manager software clusterwide. For example, a system that is running Oracle Fail Safe Manager release 3.1.1 works only with Oracle Fail Safe Server running release 3.1.1; it will not work with a server node that is running an earlier release of Oracle Fail Safe Server.

Do Not Run Windows NT Event Viewer During Oracle Fail Safe Server Installation

If you attempt to install Oracle Fail Safe Server while the Windows NT Event Viewer is running, the installation procedure may return an error indicating that it can not copy the fsus.dll file (fsja.dll on Japanese systems) and asking if you want to retry, ignore, or cancel. You can continue the installation if you stop the NT Event Viewer and then click Retry in the Oracle Fail Safe error message window.

Oracle Fail Safe Server

This section includes topics about Oracle Fail Safe Server.

Oracle Fail Safe Server and Microsoft Cluster Server Could Run Under Different Accounts

When your cluster was first configured and Microsoft Cluster Server was first installed, it was installed under a Windows NT user account.

Oracle Fail Safe Server runs as a Windows NT service under a domain user account (not the system account) that has Administrator privileges on all cluster nodes. When you install Oracle Fail Safe Server, you are instructed to provide a user name and password combination for a user account that has the required privileges. This account does not have to be the same account that Microsoft Cluster Server was installed under.
Is Alive polling is performed using the Windows NT account that Microsoft Cluster Server is running under, not the account that Oracle Fail Safe Server is running under.

If Oracle Fail Safe Server and Microsoft Cluster Server are running in separate accounts, you must add both accounts to the local ORA_DBA or ORA_<SID>_DBA NT group on all cluster nodes.

**Change in Behavior When Adding a Resource to a Group**

Prior to release 3.1.1, when adding a resource to a group, Oracle Fail Safe always returned the group to the first node being configured. For example, when adding an Oracle database to a group, the Add Resource to Group operation would always start on the node of the standalone database. After configuring the other nodes, the Add Resource to Group operation would return the database to the original node.

This behavior was changed in release 3.1.1. Now, after the resource has been added to the group, the group is moved to the first available node in the preferred nodes list. If the preferred nodes list for the group is empty (indicating that the current node is the preferred owner node), the group will remain on the last node configured.

**Oracle Fail Safe Manager**

This section includes topics about Oracle Fail Safe Manager.

**Oracle Fail Safe Manager Requires a User Name and Password When Run on Windows 2000**

Due to a named pipe problem in Windows 2000, you must supply a user name and password when you log on to Oracle Fail Safe Manager running on a Windows 2000 system.

If you log on to Oracle Fail Safe Manager running on any other system, you are not required to specify the user name and password, if your user account has appropriate privileges.

**Change in FSCMD OFFLINERESOURCE Command**

In versions of Oracle Fail Safe prior to release 3.1.1, when users did not specify the /OFFLINE qualifier for a database resource in the FSCMD resource, the default "Normal" was taken. Starting with release 3.1.1, the default value is "Immediate".
Oracle Databases

This section includes information about Oracle databases.

Oracle Fail Safe Does Not Require a Password for the Internal Account

Oracle Fail Safe does not require you to enter the password for the database Internal account if you used OS authentication to authenticate the database user. However, you must make sure that all cluster nodes on which the database can run are configured to authenticate the user through OS authentication. Full support of OS authentication for fail-safe databases will be available in a future release.

Discovery of Standalone Oracle8i Database

To discover standalone Oracle 8i databases, Oracle Fail Safe reads the database initialization parameter file (such as init.ora), which contains parameters for the Oracle8i databases on the cluster. If the shared disk on which the database initialization parameter file resides is not online on the owner node of the standalone database, Oracle Fail Safe will not discover the standalone database. If a sample database is not being discovered, make sure the appropriate shared disk is online on the owner node.

Possible Oracle8i Database Entry Errors in Oracle Fail Safe Manager

Oracle Fail Safe discovers Oracle8i databases by matching the SERVICE_NAME parameter in the database initialization parameter file and the Net8 net service name entries in the tnsnames.ora file. If you have two databases whose SERVICE_NAME values are very similar (for example, DB817 and DB8172), where one database is standalone and the other belongs to a group, Oracle Fail Safe Manager might erroneously list both databases as standalone databases.

Create Sample Database

Oracle Fail Safe includes a Create Sample Database command that installs a preconfigured sample database on a cluster disk specified by the user. The sample database has limited functionality and is intended only for testing purposes and for use with the online Oracle Fail Safe tutorial; it should not be used for production.

The following table shows the releases of the sample databases included with Oracle Fail Safe 3.1.2, and the releases of the Oracle database that can be tested with the sample database.

<table>
<thead>
<tr>
<th>Sample Database Release</th>
<th>Used with Database Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.3.4</td>
<td>7.3.4</td>
</tr>
</tbody>
</table>
The sample database files can be installed only on a node where the appropriate release of the Oracle database server is installed. For example, if Oracle database server release 8.1.5 is installed, then only the sample database for 8.1.5 will be installed during the Oracle Fail Safe installation.

There are known limitations in using the sample databases with releases other than the release for which they were originally created. When an 8.1.5 sample database is installed for use with Oracle database server release 8.1.6, the following errors are returned when attaching to the database:

**ERROR:**
ORA-06533: PLS-908: The stored format of SYS.STANDARD is not supported by this release.

Error accessing packing DBMS_APPLICATION_INFO
**ERROR:**
ORA-06533: PLS-908: The stored format of SYS.STANDARD is not supported by this release.

The sample database feature provided by Oracle Fail Safe is to be used for testing only; to create a database for production, use the Oracle Database Configuration Assistant or create the database manually.

**Support for Archive Logs**

In Oracle8i release 8.1.5 and later, you can define an archive log destination as a service name instead of a disk location.

For example:

```
log_archive_dest_1='LOCATION=f:\<dir_name> MANDATORY REOPEN=5'
log_archive_dest_2='SERVICE=standby OPTIONAL REOPEN=120'
```

The example shows typical entries that are allowed in Oracle8i release 8.1.5 for archive log support:

- The first entry specifies a file system destination. Oracle Fail Safe will check this location to make sure that the disk used is a cluster disk and accessible to all cluster nodes.
- The second entry specifies a TNS service name entry of "standby." Oracle Fail Safe will not automatically update the TNSNAMES.ORA file on all cluster nodes. You must manually edit or add the service name entry to the TNSNAMES.ORA file on all cluster nodes.
**Standby Support**

Oracle Fail Safe supports configuring only the primary standby database on a cluster. Remote standby databases configured in either recovery mode or read-only mode cannot be configured on clusters using Oracle Fail Safe; they must run as standalone databases.

**Change in Database Listener Resource and Database Resource Dependencies**

When the Oracle Fail Safe database resource DLL tries to connect to a database, it uses the SQL*Net listener. If this connection fails, the database resource DLL uses a SQL*Net bequeath connection, which bypasses the SQL*Net listener. Therefore, the database is no longer dependent on the database listener for Oracle Fail Safe to connect to the database.

If the SQL*Net listener resource fails, it will be restarted based on its resource restart policy. Due to the removal of the dependency between the database and the database listener, the database will not be taken offline if the listener fails.

**Problem with Large listener.log Files**

Due to the number of database connections involved in IsAlive polling, the listener.log file for the Oracle Fail Safe listener can become very large very quickly. You can solve this problem in one of two ways:

- Periodically delete the listener.log file. You can delete the file without stopping the listener.
- In the listener.ora file, set the `LOGGING_<listener name>` parameter to `OFF`. Be sure the listener whose logging you turn off is the Oracle Fail Safe listener.

**Standalone Database Resources No Longer Restarted Unconditionally During a Verify Operation**

Oracle Fail Safe no longer automatically starts and stops database instances during a Verify Standalone Database operation.

**User Name for Database Must Be Internal**

To ensure the success of all Oracle Fail Safe operations, the database user name must be "Internal".

**Oracle Reports**

This section includes information about Oracle Reports.
Inconsistent NAMES.DEFAULT_DOMAIN Parameter Might Cause Oracle Reports Server to Fail

The value for the NET.ORA parameter NAMES.DEFAULT_DOMAIN must be the same across all Oracle homes in the cluster. If it is not, you may experience problems with Oracle Reports Server resources. For example, an Add Oracle Reports Server to Group operation might fail or a Verify Group operation might fail if the group contains an Oracle Reports Server.

Incorrect Message When You Verify a Group Containing an Oracle Reports Server

When you verify a group that contains an Oracle Reports Server, the following message may be displayed when the service name for the Oracle Reports Server exists and is correct:

FS-10693: Oracle Reports Server <report-name> does not exist in <Oracle_Home>\Net80\Admin\Tnsnames.ora on node <node-name>. Do you want to create it with default port 9100?

This message is displayed each time you verify the group that contains the Oracle Reports Server regardless of how you respond to the error message query.

Oracle Forms Load Balancer Server

This section includes information about Oracle Forms Load Balancer Server.

Validate the FormsWeb.cfg file After Adding an Oracle Forms Load Balancer Server Resource

After adding an Oracle Forms Load Balancer Server resource to a group, validate the MetricServerPort and ServerPort parameters in the formsweb.cfg file, which is used by the Forms CGI executable. The file is located at <Oracle_Home>\Forms60\formsweb.cfg. The MetricServerPort parameter that you specified should have the same value as the RequestPort startup parameter specified when you added the Oracle Forms Load Balancer Server resource. The ServerPort parameter should have the same value as the startup parameter for Oracle Forms Server.

Oracle Application Server

This section includes information about Oracle Application Server.
Error Accessing Oracle Application Server Resource Properties

If you select an Oracle Application Server resource (as opposed to an Oracle Application Server Web listener resource) and attempt to access its properties, you will receive the following error:

ERROR:
FS-10880: Error calling method Init of FscOASWebListener class.

This limitation is minor because an Oracle Application Server resource does not have any noncluster properties.

Adding a Node to a Cluster That Contains an Oracle Application Server Web Listener

When you add a new node to the cluster and run the Verify Group operation, Oracle Fail Safe replicates the resource configuration for all resources in the group on the new cluster node. However, if you verify a group containing an Oracle Application Server Web listener, Oracle Fail Safe does not replicate the listener configuration on the new cluster node.

Therefore, if you add a new node to the cluster and want that node to be a possible owner node for an Oracle Application Server Web listener, you must do the following:

1. Remove the Oracle Application Server Web listener from the group. When you perform the Remove operation, make sure that a standalone Oracle Application Server Web listener is left on at least one cluster node.

2. Add the new node to the cluster (as described in the Oracle Fail Safe Installation Guide). Be sure to include the Oracle Application Server component as part of the Oracle Fail Safe installation.

3. Add the standalone Oracle Application Server Web listener back into the group. Oracle Fail Safe will configure it on the new cluster node.

Workaround Recommended in Oracle Application Server 4.0.8.1 Release Notes (December 1999) Is Not Recommended for Oracle Fail Safe Environments

In the section titled "Latest Updates" of the Oracle Application Server 4.0.8.1 Release Notes (December 1999), the documentation states that by applying a workaround you can install Oracle Application Server release 4.0.8.1 on the same system as an Oracle database that is a release prior to 8.0 or is release 8.1 or later. (Previous versions of the Oracle Application Server Release Notes stated that these combinations do not work together on the same machine.) This workaround is not recommended for use in Oracle Fail Safe environments.
The workaround recommended in the Oracle Application Server Release Notes states that if the database and Oracle Application Server are launched with different path variables, they will function correctly. The release note describes how to make path and service changes to accomplish this goal. (See the Oracle Application Server 4.0.8.1 Release Notes (December 1999) for details on the workaround.)

If you have performed this workaround, you have the following configuration:

- Oracle Application Server 4.0.8.1 installed under an Oracle Application Server administrator account
- Oracle database server that is a release prior to 8.0 or is a release 8.1 or later installed under the default system administrator account

However, if you attempt to use this configuration in an Oracle Fail Safe 3.0.3 or higher environment, you get the following errors when you attempt to add an Oracle Application Server Web listener to a group:

- ERROR : FS-10726: Resource OAS<Oracle Home><web listener> is in a failed state.
- ERROR : FS-10012: Failed to bring the cluster resource OAS<Oracle Home><web listener> online.
- ERROR : FS-10778: The Oracle Web Listener resource provider failed to configure the cluster resource <web listener>.

The solution to this problem is to not do (or undo) the path and service changes that are recommended in the Oracle Application Server release notes.

However, if you do not make the path and service changes recommended in the Oracle Application Server Release Notes, then Oracle Application Server 4.0.8.1 and an Oracle database server that is a release prior to 8.0 or release 8.1 or higher will not work on the same machine in an Oracle Fail Safe 3.0.3 or higher environment. If you have these three products (in the stated versions), Oracle Corporation recommends that you do one of the following:

- Use two systems (one in the middle-tier for Oracle Application Server and Oracle Fail Safe, and one in the back-end tier for Oracle database server and Oracle Fail Safe).
- Use combinations of the Oracle database server releases and Oracle Application Server releases that work together without requiring the workaround suggested in the Oracle Application Server release notes involving path and service changes.
**Oracle Application Server in Online Pending State**

After a node is rebooted, Oracle Fail Safe starts all fail-safe resources owned by that node. It can take up to 5 minutes for an Oracle Application Server to start. While the Oracle Application Server is starting, the group that contains it will be in the online pending state (as seen through MSCS Cluster Administrator).

**Oracle Application Server Must Be Installed in the Primary Oracle Home**

In most cases, the Verify Cluster command correctly detects whether or not the Oracle home where Oracle Application Server is installed is the primary Oracle home on all cluster nodes. However, the Verify Cluster command does not detect the case where Oracle Server 8.x is installed in the primary Oracle home, rather than Oracle Application Server.

Therefore, Oracle Corporation recommends the following:

- After you install all Oracle products on all cluster nodes, but before you configure Oracle Application Server with Oracle Fail Safe, use the Oracle Home Selector to confirm that the Oracle home where Oracle Application Server is installed is the primary Oracle home on all cluster nodes.

- Check that the home where Oracle Application Server is installed is the primary home after you install any Oracle products in the future.

A quick method for determining whether or not the primary Oracle home is set correctly is to issue the `owsctl -V` command in the Windows command window. If the primary home is not set correctly, one of the following occurs:

- The command hangs.
- An `owsctl.exe Application Error` dialog box opens.
- The "Error initializing CORE" message is returned.

**Oracle Fail Safe Cannot Change Oracle Application Server Web Listener Properties**

Oracle Fail Safe does not provide a way to modify existing Oracle Application Server Web listener properties. To modify the root directory, initial file, or virtual directories of an existing Oracle Application Server Web listener, use Oracle Application Server Manager. The changed properties will not take effect until the listener is restarted.
Verify Group Command Does Not Fix Problems with Oracle Application Server Web Listener

The Verify Group command detects problems with the Oracle Application Server Web listener resource, but does not attempt to fix them. If an Oracle Application Server Web listener resource is damaged, Oracle Corporation recommends that you delete the resource and then re-create it.

Use Oracle Fail Safe Manager to remove the damaged Oracle Application Server Web listener resource from the group, and then delete it from the cluster. If you receive an error when you try to remove the resource from the group (such that the Oracle Application Server Web listener is still in the group), then use MSCS Cluster Administrator to delete the resource from the group, and then use Oracle Application Server Manager to delete the Web listener from each cluster node.

Oracle Fail Safe Sets the Common Gateway Interface (CGI) Execution Permissions to NR

When you add an Oracle Application Server Web listener to a group, Oracle Fail Safe sets the common gateway interface (CGI) execution permissions of the virtual directories to NR. (When execution permissions are set to NR, users cannot execute CGI applications from the virtual directories or their subdirectories.) You can modify the CGI execution permissions of a virtual directory with Oracle Application Server Manager. If you use Oracle Application Server and Oracle Reports Server to display Web reports, you must set the CGI execution permissions of the web-cgi directory to CR. (When execution permissions are set to CR, users can execute CGI applications in the web-cgi directory and its subdirectories.)

Do Not Configure the Node Manager or Admin Web Listener for High Availability

When you install Oracle Application Server on a node, it automatically creates Web listeners called Node Manager and Admin. These listeners are used by Oracle Application Server Manager to accept Web listener configuration changes, such as changes to the CGI execution permissions of a virtual directory.

Because Oracle Fail Safe resets the CGI execution permissions of a virtual directory to NR when you add an Oracle Application Server to a group, you should not configure the Node Manager or Admin Web listener for high availability. If you add the Node Manager or Admin Web listener to a group, its CGI execution permissions will be set to NR, and it will not be able to execute its CGI applications. Thus, you will not be able to use Oracle Application Server Manager to make configuration changes to any Web listeners, including changing the CGI execution permissions for the Node Manager or Admin Web listener back to CR.
Because the Node Manager and Admin Web listeners should be used only by Oracle Application Server administrators and not users, the inability to configure them for high availability is not an issue.

**Modified certs.db File Is Not Copied to Other Cluster Nodes**

If you add a standalone Oracle Application Server release 4.0.8 Web listener to a group, and that standalone Web listener currently exists on one node only, Oracle Fail Safe creates a copy of it on the other nodes. However, the newly created Web listener will have the default certs.db file, not a copy of the original certs.db file of the standalone Web listener. (The certs.db file is new for Oracle Application Server release 4.0.8. It contains a listener’s certificates for accessing the Oracle Application Server.) You can use the Oracle Application Server Manager to modify the certs.db file of the newly created Web listener. This is a concern only if you changed the certs.db file for the standalone Web listener.

**Oracle Fail Safe Uses a Default Standalone Port When You Remove an Oracle Application Server Web Listener from a Group**

If you remove an Oracle Application Server Web listener from a group and do not delete the NT service, Oracle Fail Safe configures the standalone listener to listen on port 8973 on the node’s IP address/network name. Oracle Fail Safe does not prompt you for a different port, nor does it check if port 8973 is in use on the node. If necessary, use the Oracle Application Server Manager to reconfigure the standalone listener to listen on a different port.

**Incorrect Messages Are Returned for Attempts to Delete Listeners Created During Oracle Application Server Installation**

If you remove the special Oracle Application Server node, Admin, or default Web listeners from a group and select ‘yes’ to the question regarding deleting the NT service from the node, Oracle Fail Safe correctly returns the warning "Oracle Fail Safe will not delete the special OAS Web listener <name>." (These listeners are part of the Oracle Application Server installation and are required by Oracle Application Server. This is appropriate software behavior.) However, Oracle Fail Safe also returns the message "Deleted NT service <name>." This second message is incorrect; the NT service has not been deleted.

**No Message Is Returned for Attempts to Delete Listeners Created During Oracle Application Server Installation**

If you issue the Delete command in an attempt to delete the special node, Admin, or default Oracle Application Server Web listeners (created during the Oracle Application Server installation), no message is returned. Oracle
Fail Safe Manager refreshes the tree view, and the listener is still listed among the standalone resources. The failure to delete the special Oracle Application Server Web listeners is correct. (These listeners are part of the Oracle Application Server installation and are required by Oracle Application Server. This is appropriate software behavior.) However, Oracle Fail Safe should return a message to indicate that the requested operation was not performed.

**Oracle MTS Service**

This section includes information about Oracle MTS Service.

**Add Oracle MTS to Group Operation Fails**

If the Add Oracle MTS Service to Group operation fails, it may be due to a problem with the value for LAST_HOME in the Windows registry. If you attempt to add an Oracle MTS Service to a group and the LAST_HOME entry for HKEY_LOCAL_MACHINE/SOFTWARE/ORACLE/ALL_HOMES is not equal to the highest Oracle home number on your system, then the Add Oracle MTS Service to Group operation will fail and you will receive the following messages:

- FS-10778: The Oracle MTS Service resource provider failed to configure the cluster resource <resource-name>
- FS-10618: Failed to change the configuration for NT service <service-name>
- 0x424: The specified service does not exist as an installed service

For example, if you have HOME0, HOME1, and HOME2 on your system, the value for LAST_HOME must be 2 for the Add Oracle MTS Service to Group operation to work. To fix the problem, change the value of LAST_HOME to match the highest Oracle home number on the local machine and rerun the Add MTS Service to Group Wizard.

**Oracle Database Release 8.1.6 Requires a Patch**

The Oracle Fail Safe support for Oracle MTS Services requires a patch to be applied to the Oracle 8.1.6 database server. If you do not have information on obtaining the Oracle 8.1.6 database server patch, perform the following steps after installing Oracle Fail Safe 3.1.2:

1. Stop the Oracle MTS Services running on the machine.
2. Rename the copy of oraps0.exe in the bin directory of the Oracle home where Oracle MTS Service is installed.
3. Copy oraps0.exe from `<Oracle_Home1>`\fs\fssvr\bin to `<Oracle_Home2>`\bin, where `<Oracle_Home1>` is the Oracle home directory
where Oracle Fail Safe is installed and `<Oracle_Home2>` is the Oracle home directory where Oracle MTS Service is installed.

The new oraps0.exe will allow you to make Oracle MTS Services fail-safe.

**Disk Resources**

Oracle Fail Safe allows the use of EMC GeoSpan disks. However, if you attempt to add a resource to a group and an EMC GeoSpan disk used by the resource is not already in that group, then Oracle Fail Safe returns the error FS-10202 and rolls back the operation.

If this occurs, add the resource to the group that already contains the EMC GeoSpan disk that the resource requires.

**Clients and Applications**

This section includes information about clients and applications that access resources that have been made highly available.

**Problem with Transparent Application Failover in Oracle Server 8.1.6**

There is a problem if failover occurs during a SELECT operation if you are using the Oracle Server 8.1.6 transparent application failover (TAF) feature with the RETRIES and DELAY parameters in the FAILOVER_MODE of the TNS service name. After the database fails over, one row is not fetched, and instead of the data, an extra blank row is inserted into the results table.

A bug (1222904) has been filed for this problem against Oracle Server 8.1.6. You can either monitor the bug for the resolution of this problem or wait until a fix is made available by an Oracle Server 8.1.6 patch.

**Oracle8 OCI TAF Feature and Releases of Oracle Prior to 8.0.5.2**

The Oracle8 OCI transparent application failover (TAF) feature may not work correctly during failback for Oracle database release 7.3.4. Although clients and applications will automatically reconnect after the initial failover, they may not automatically reconnect after failing back to another node. The problem is fixed in the Oracle 8.0.6, 8.1.5, 8.1.6, and 8.1.7 database releases.

**Oracle Enterprise Manager Integration**

This section includes information about integrating Oracle Fail Safe with Oracle Enterprise Manager.
Discovery of Virtual Hosts with Oracle Intelligent Agent 8.1.7

To discover an Oracle Fail Safe virtual host using Oracle Intelligent Agent 8.1.7:

1. In Oracle Enterprise Manager, right-click on "Nodes."
2. Select "Discover nodes."
3. Enter the virtual hostname without the domain name.

If you enter the virtual hostname with the domain name, you will get an error. This restriction only applies to the first time you discover a virtual host. Subsequent times, entering the virtual hostname with or without the domain name will discover both.

Oracle Intelligent Agent Release 8.1.7 Is the Only Supported Release

Oracle Fail Safe 3.1.2 supports Oracle Intelligent Agent release 8.1.7 only. Oracle Intelligent Agent release 8.1.7 supports all Oracle database releases that Oracle Fail Safe 3.1.2 supports, as well as addressing some of the limitations of the Oracle Intelligent Agent releases 8.1.5 and 8.1.6.

Oracle Intelligent Agent release 8.1.7 is available with the Oracle 8.1.7 database or as a standalone product in the Oracle 8.1.7 CD pack. As with all 8.1.7 products, Oracle Intelligent Agent can be installed in an Oracle home that contains only other 8.1.7 products, or in its own Oracle home.

When you add an Intelligent Agent resource to a group, you select the agent from the 8.1.7 home.

Partial Support of JobOut Subdirectory

Oracle Intelligent Agent release 8.1.7 deposits its jobs output files into a directory called JobOut. For highly-available intelligent agents, the JobOut directory is a subdirectory under the agent’s ConfigPath directory on the cluster disk. The intelligent agent requires the JobOut subdirectory to run jobs.

When creating an intelligent agent and adding it to a group, Oracle Fail Safe 3.1.2 creates the JobOut subdirectory on the cluster disk. However, when verifying a group with a highly-available intelligent agent in it, Oracle Fail Safe 3.1.2 does not verify that the JobOut subdirectory exists. In addition, when changing a highly-available intelligent agent’s cluster disk, Oracle Fail Safe 3.1.2 does not create a JobOut subdirectory on the new disk, nor does it remove the JobOut subdirectory on the old disk.

Fail-Safe Database Discovered as Standalone Database on Physical Nodes

When you view standalone databases on physical nodes, you may see fail-safe databases that are online on the physical node being discovered.
This problem appears on systems running Windows NT 4.0 Service Pack 3, 5, or 6a.

If there is an Intelligent Agent resource in the group, then databases in the group will not be discovered under the physical nodes. The exception to this case is when the database uses more than one virtual address. If the first virtual address used in the listener.ora and tnsnames.ora files for the database is not selected for use by the agent, then the databases in the group will be discovered under the physical nodes.

**Default Intelligent Agent of Physical Node Is No Longer Restarted by Fail Safe**

Prior to Oracle Fail Safe 3.1, the default intelligent agent of a physical node was restarted during the Create Sample Database, Delete Sample Database, Add Database to Group, and Remove Database from Group operations. Starting with Oracle Fail Safe 3.1, the default Intelligent Agent of a physical node is no longer automatically restarted. If you need an updated list of databases under the physical nodes, restart the default agent manually.

**Documentation Updated for This Release**

The following documentation has been updated for this release.

- *Oracle Fail Safe Concepts and Administration Guide*
- *Oracle Fail Safe Release Notes*
- *Oracle Fail Safe Installation Guide*
- *Oracle Fail Safe Error Messages*
- Oracle Fail Safe Tutorial
- Oracle Fail Safe Help
- Oracle Fail Safe Quick Tour

The documentation that comes with the kit is provided in HTML and PDF online formats. Viewing the PDF files requires Adobe Acrobat Reader 3.0 or later. You can download the newest version from the Adobe Web site at:

http://www.adobe.com/prodindex/acrobat/readstep.html

**Documentation Errors**

This section corrects known errors in the Oracle Fail Safe documentation set for release 3.1.2.
Oracle Fail Safe Concepts and Administration Guide

- The Oracle Fail Safe Concepts and Administration Guide for releases 3.1.1 and 3.1.2 indicate that Oracle Fail Safe does not support the use of dynamic HTML files with Oracle Forms Server 6i. This is incorrect; Oracle Fail Safe supports the use of static and dynamic HTML files with Oracle Forms Server 6i.

- Section 7.11.1 of the Oracle Fail Safe Concepts and Administration Guide indicates that an error handling script is called according to the following guidelines:

```
FsDbError.bat <error code> <TNS service name> <SID> <parameter file spec>
```

This is incorrect; the error handling script should be called according to the following guidelines:

```
FsDbError.bat <error code> <database name> <SID> <TNS service name> <parameter file spec>
```

Oracle Fail Safe Quick Tour

- In step 4 of the Oracle Fail Safe Quick Tour lesson entitled Groups and Virtual Addresses, the image incorrectly implies that Oracle Fail Safe creates a dependency between the database and the SQL*Net listener. Beginning with release 3.1, Oracle Fail Safe no longer creates a dependency between the database and the SQL*Net listener.

Obsolete Features

This section describes Oracle Fail Safe features that are now obsolete.

- The Migrate Group command, available with Oracle Fail Safe releases 2.1.2 and 2.1.3, is not available beginning with release 3.0.3.

- The GR_MIGRATE trace flag (which captured tracing information when you used the Migrate operation) is obsolete.

- The wizard to facilitate making Microsoft Internet Information Server (IIS) highly available is no longer provided. Use Microsoft Cluster Administrator to configure IIS.

- The View Event Status command is no longer provided. Use the Windows Event Viewer instead.

Software Errors Fixed

Software errors that have been fixed since the last release of Oracle Fail Safe are described in the following list:
- Previously, under certain conditions, the Verify Group command returned incorrect errors. This problem has been fixed.

- During the security setup portion of the installation, you supply the user name and password of a Windows NT account. In previous releases of Oracle Fail Safe, if the user account belonged to too many Windows NT groups, the operation could fail to validate the user account. This problem has been fixed.