

Disaster Recovery and High Availability Solutions for Oracle using SteelEye LifeKeeper

Index

<i>Introduction</i>	<i>Page 2</i>
<i>High Availability and Disaster Recovery for Oracle</i>	<i>Page 2</i>
<i>Protection for the Oracle Environment</i>	<i>Page 3</i>
<i>Configuration Considerations</i>	<i>Page 4</i>
<i>Active/Active</i>	<i>Page 5</i>
<i>N+1 Configuration</i>	<i>Page 5</i>
<i>Off-site Disaster Recovery</i>	<i>Page 6</i>
<i>Combining Disaster Recovery and High Availability</i>	<i>Page 6</i>
<i>Network Considerations</i>	<i>Page 7</i>
<i>Summary</i>	<i>Page 7</i>
<i>Further Information</i>	<i>Page 7</i>

Abstract

This white paper describes how to use SteelEye LifeKeeper to provide high availability and disaster recovery protection for Oracle in both Windows and Linux-based environments.

All solutions mentioned in this white paper are available today from Open Minds High Availability Solutions.

Many more solutions are possible than are given in this white paper, so if what you are trying to achieve is not shown in this document, then please feel free to contact us to discuss your requirements.

Introduction

Enterprises, both large and small, rely on Oracle database solutions for business critical applications including data warehouses, e-commerce applications, financial systems, supply-chain management and business intelligence systems. These environments require high availability protection against application or server downtime. To date, however, ensuring 24/7 availability has required high costs, numerous redundant systems and a dedicated IT staff.

Traditionally only larger enterprises have been able to justify high availability solutions, as they required high end custom hardware or proprietary operating systems, or a mixture of both. Our solution is able to escape from both of these constraints, and allows for any Intel hardware to be used, along with the Microsoft Windows or Linux family of operating systems.

High Availability and Disaster Recovery for Oracle

The term High Availability refers to a systems ability to recover from failure, whether this is hardware or software related, in order to provide continuous service to the user. High Availability systems often allow for a small window of downtime. After a failure has been detected, the host locally recovers from the failure, or a fail-over takes place, transferring one servers tasks to another server. The window of downtime can vary from a few seconds to minutes, depending upon the application and failure. In the case of Oracle servers, recovery time, depending on the number of users, can be as low as 1 minute.

The term Disaster Recovery refers to the ability of a server or service to recover from a failure where the servers are located across 2 separate physical sites. This distance is used to protect critical servers against site disasters such as fires.

Both high availability and disaster recovery are a part of the SteelEye LifeKeeper solution. As failover can take place on a local or remote server. There is also a combined 3-node solution that incorporates a local and a remote failover.

The LifeKeeper Oracle Protection Suite for Windows or Linux recovers Oracle databases and services after hardware or software failure. After a failure has been detected, the Oracle database and services are recovered on a designated backup server. The backup server can be located on the same LAN as the active Oracle server, or on a WAN to provide disaster recovery.

High Availability and Disaster Recovery for Oracle continued

It can work equally well with and without shared storage. Features of SteelEye's implementation for an Oracle Fault Resilient solution include:

- LifeKeeper works on all versions of Windows and Linux, there is no requirement for the high end, Enterprise level versions of the OS.
- LifeKeeper works on all versions of Oracle including Oracle 8i, 9i and 10g, and it does not require Oracle RAC or Microsoft Cluster Server.
- LifeKeeper does not require shared storage (e.g. SAN, Shared SCSI or a NAS)
- LifeKeeper provides for a disaster recovery solution, giving ultimate protection to important data.
- LifeKeeper allows applications other than Oracle to run on a protected server. These applications do not need to be cluster aware.
- LifeKeeper returns the failed server back into the cluster seamlessly by re-synchronising data and making the failed server the backup server.

LifeKeeper protects, not just from hardware failure but also the Oracle services. Therefore, hardware resilience and software resilience is achieved via the LifeKeeper Oracle solution. The solution has been deployed worldwide and in the UK we have customers running the Oracle 8i, 9i and 10g solution.

Protection for the Oracle Environment

Oracle services monitored

LifeKeeper actively monitors and protects all resources required by Oracle databases, and actively checks that the database itself is available, resulting in responsive failover to another node within the cluster if there are problems (e.g. faulty network cable, disk failure or server hang).

LifeKeeper monitors the Oracle database, listeners, disks and networks, if a problem is discovered with any one of these LifeKeeper will attempt to resolve the problem by restarting the database. If the problem persists fail over to the designated back-up server takes place.

The administrator will be informed of the failure and will be free to repair the service safe in the knowledge that the back-up server has taken over the primary servers responsibilities, in most cases users will not even realise a failure as occurred.

Protection for the Oracle Environment continued

No need for downtime during upgrades and maintenance

As well as being useful in preventing system disasters, LifeKeeper can also be used to assist system upgrades or for installing new hardware and/or applications. This is possible as the service can be manually switched over from one node to another at will, allowing the inactive node to be upgraded/repaired. The administrator can then check that the newly upgraded node works, and if not switch back to using the other system. This reduces the need to schedule downtime for common maintenance tasks and upgrades, helping to enhance the availability and reliability of the service as a whole.

Configuration Considerations

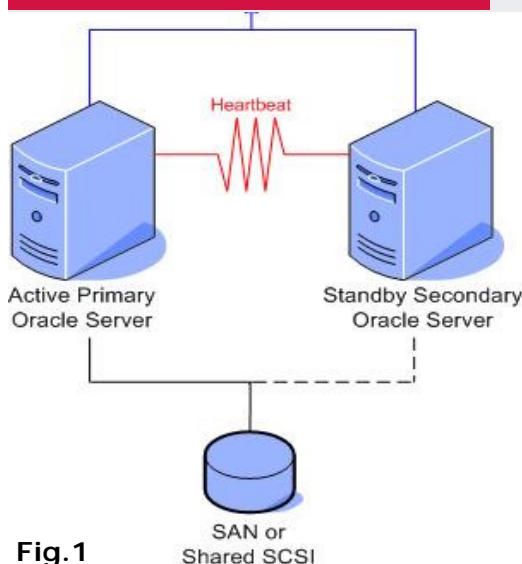


Fig.1

Active/Standby Configuration

Using Shared Storage

Oracle can be installed on shared storage or on both the active and back-up servers.

In fig.1 the Active server has access to the shared storage, while the back-up server is locked out. Oracle is running on the active server, and the heartbeat between the nodes is monitoring the database.

LifeKeeper manages access to the shared storage, ensuring that only one server has access at any one time.

If a problem occurs, for example if the power fails to the primary server this would be detected by LifeKeeper, a restart would not be possible, so a failover would occur. LifeKeeper then allows the back-up server access to the shared storage, and the back-up server assumes the responsibilities of the primary server.

Failover is almost transparent to users as they can continue to access the database without reconfiguration due to the automated migration of a floating IP address or automated update of DNS settings in a Windows environment.

Active/Standby Configuration

Using Data Replication

The processes are very similar in a data replication environment. However the database is stored locally on the active server and mirrored onto the backup server. Monitoring and failover are the same as above. In the event of a failover the data replication stops, when the cause of the failover is resolved any data that has changed will be updated on the primary server with a partial resynchronisation and service can resume as normal.

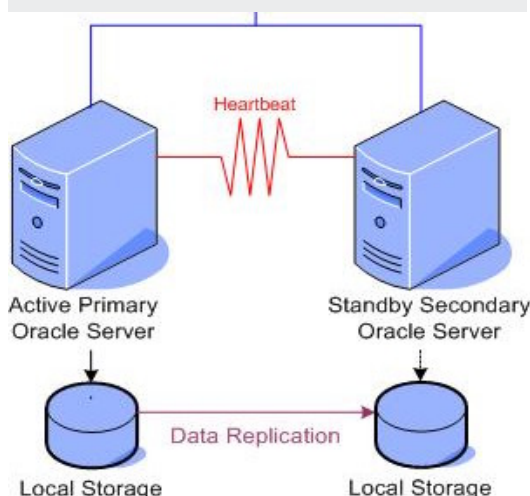


Fig.2

Configuration Considerations

Active/Active Configuration

Using Shared Storage

The active/active configuration allows for the most efficient use of hardware resources. Two servers each running different instances of applications act as back-up to each other. If the Primary Oracle server fails in fig.3 the other server assumes its responsibilities, as well as continuing with its original tasks. The same would occur if the Primary server for the other application encountered a problem.

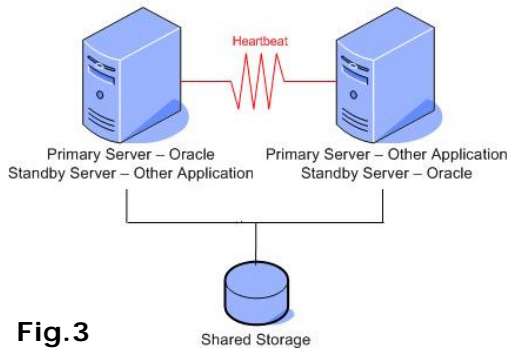


Fig.3

Using Data Replication

The active/active configuration can also be implemented in a data replication environment.

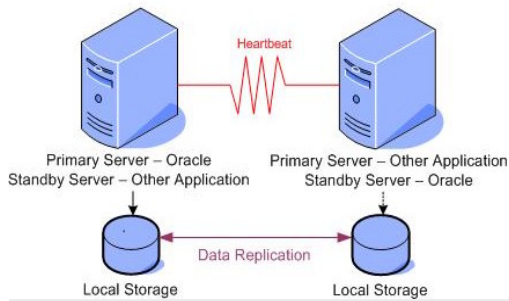
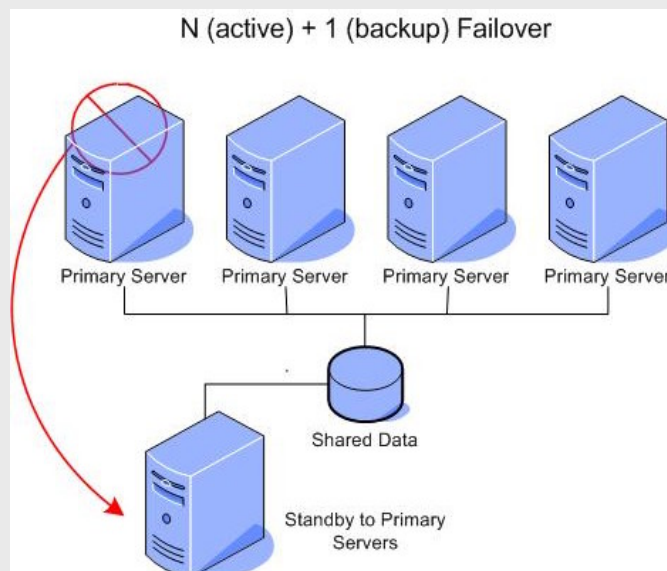


Fig.4

N + 1 Configuration

It is also possible to have a number of servers all being protected by one standby server. The financial advantages of this solution are significant as it reduces licence and hardware costs.

For example, if 4 servers are protected by one backup server (as shown in the diagram), there will only be 5 servers in total, rather than 8 servers if each server had its own separate backup server. This results in a reduction in costs of hardware, licences, support and maintenance. This configuration can also operate in a Data replication environment.



Off-site Disaster Recovery

It is also possible to have a 2-node failover over a Wide Area Network. This allows organizations to deploy a disaster recovery system relatively inexpensively.

The Oracle servers are configured in an active/standby configuration. As you can see in fig.5, one Oracle server is located in an off site data centre, while the primary Oracle server is located on the main premises. Should the local Oracle server fail, LifeKeeper will move the service to the data centre. This fail over will be seamless to clients, who will continue connecting as normal.

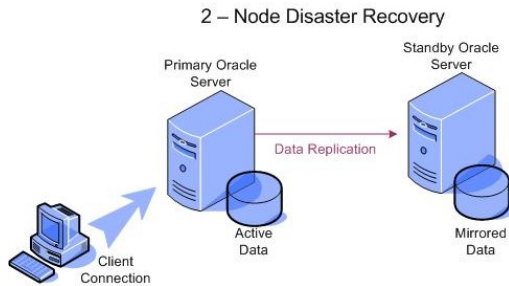


Fig.5

Combining Disaster Recovery and High Availability

The 3-node solution offers the advantages of a local failover and disaster recovery.

This solution offers the benefits of :

- Minimal disruption is experienced by users when a server or application failure is experienced.
- Local failover can be used for administration purposes such as upgrades and maintenance.
- The remote server is only used for site disasters.
- WAN replication can be stopped during peak traffic and restarted as required.
- If the WAN link is unavailable, the local copy of the data is still available and Oracle is still protected.

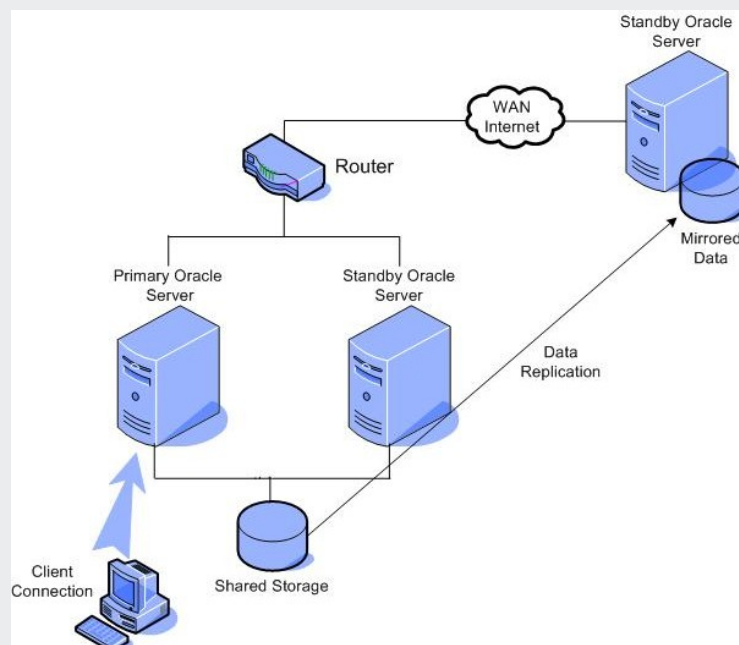


Fig.6

Networking Considerations

The data replication software replicates at block level. It is therefore unaware of files and how much of the disk is actually being used. There is no replication of white space and only changed data is replicated. This minimises the traffic on the network. In addition, if the network speed is an issue at certain times of the day, it is possible to pause the mirror at peak traffic times, when un-paused a partial resynchronisation will take place, replicating the altered data, therefore completing the mirror.

In the event of a disaster recovery solution being deployed, where the nodes are separated by some distance, an Asynchronous mirror can be used, which improves performance on the active node (but does increase the chance of data loss). The asynchronous mirroring can be undertaken over lower speed links if necessary – unfortunately it is hard to estimate what speed of link is required for each customer due to differing requirements and usage patterns. As mentioned above, only write requests are mirrored to the remote server, so if a large amount of the activity is reading then a low speed link may be feasible.

In a Low Bandwidth Environment

Open Minds have customers operating on links from 1mbit/s to 100mbit/s for disaster recovery solutions.

Various levels of compression and bandwidth throttling are also available in order to facilitate low-bandwidth environments.

In some instances where there is a high volume of data and a comparatively low bandwidth available it is recommended that the initial synchronisation is performed locally over a high-speed link. Once this is complete the back-up server can be moved to the disaster recovery site. Only a partial resynchronisation would be

In Summary

Oracle servers can be recovered in many different scenarios. Data Replication is required where there is no access to shared storage, or where a disaster recovery solution is required.

There is no requirement for Oracle Enterprise Edition and additional applications (whether they are Oracle based or not) can easily be protected, these additional applications do not need to be cluster aware.

This white paper provides a rough guide to the solutions available, there is of course, no substitute for seeing the solution and discussing your requirements with one of our solution architects, so please feel free to contact us and we would be happy to talk through your requirements.

Contact Information

For further information regarding this or any other white paper please do not hesitate to contact Open Minds High Availability Solutions

Phone: +44 (0) 845 345 3943
+44 (0) 121 313 3943

Email: sales@openminds.co.uk

Web: <http://www.openminds.co.uk>

