Oracle Database Protection by Spitfire StoreSafe

Bloombase
Least Invasive Security

Bloombase
Least Invasive Security

Document No.

Contents

Introduction

Digital assets including financial reports, legal documents, private human resources information, confidential contracts and sensitive user data are invaluable properties of a corporation. A business cannot risk losing these information, both confidentiality and non-repudiation. Nevertheless, the Internet has becoming more pervasive, security attacks have grown. News and reports have revealed millions of dollars of loss in various enterprises and organizations due to security breaches.

Data protection at the persistence layer used to be an uncommon subject in information technology industry. Persistence data, in the old days, are assumed safely kept and stored in highly secure data centers with effective physical access control and close surveillance. However, trends in the industry in backup, archive and high availability with an aim to safeguard data from the worst attack and be responsive to rescues, keeping the enterprise core system running non-stop, have opened up chances confidential data get disclosed and tampered by unauthorized parties.

Numerous security compliance and standards including Sarbanes Oxley, Gramm-Leach-Bliley Act and Personal Data Privacy Ordinance have raised enterprises' awareness of securing their core business and customer data. However, persistence data protection is technically a difficult subject. One has to prepare for additional system complexity, loss of performance, at the same time, maintaining the same level of stability and scalability, and most important of all, be highly secure, hacker-proof rather than exposing more security loopholes.

Core business data of an enterprise constitutes a major segment of assets that a corporation possesses. Customer data, marketing strategies, intellectual properties in form of source codes and business logic, sales history and prediction figures, and other decision support numerical analysis as result of data-mining may often bury forward looking intelligence that in some sense have very high future value when put into good use.

A number of factors put persistence data at risk

- Office automation
- Company insider
- Information lifecycle management (ILM) and backup/restore (BURA)

- Disaster recovery (DR) and high availability (HA)
- Growth of storage data
- Storage consolidation
- Inter-corporate application integration
- Storage device
- System backdoors
- Viruses, worms and spyware
- Remote accessibility
- Hardware disposal handling
- Outsourcing
- Effective perimeter protection

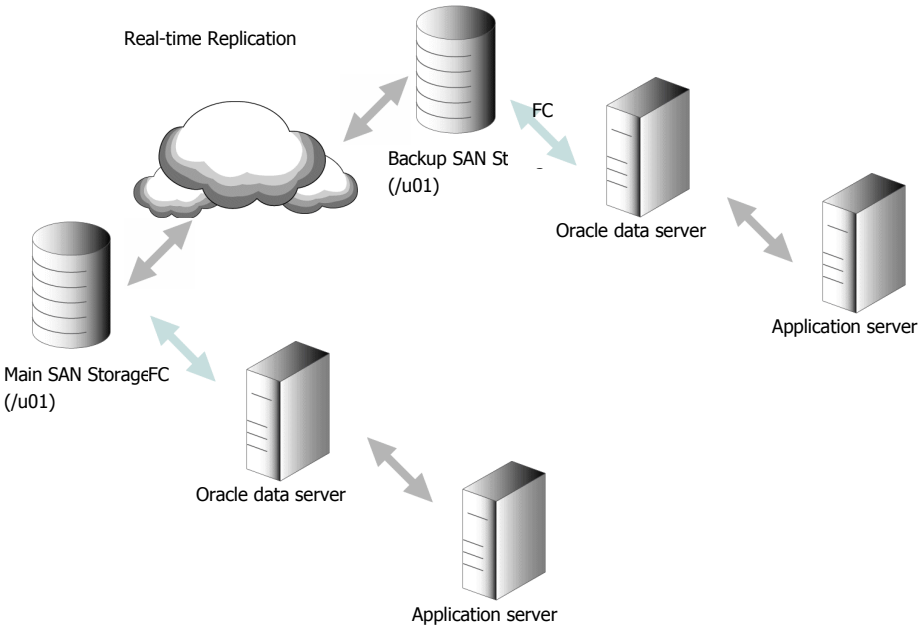
This paper studies how Spitfire StoreSafe enterprise storage security server helps to fill in the missing puzzle of enterprise data threats and serves as a cookbook for a number of typical applications in today's enterprise computing environment.

Database and Real-time Replication Protection

Problem

A government security bureau processes large volume of trade declarations which needs to be secured as they are persisted into Oracle databases. As their system has been on production for years, it is required that data security has to be introduced without requiring application changes. Again, the system cannot tolerate throughput degradation by more than 30%.

Apart from the production system, they have another backup system which receives delta changes of the master database timely. At any one time the production system goes down, this resilience system will be switched over as the master system and resumes service.



Their system runs on a high-end enterprise class Sun Microsystems Sun Fire E6900 which is highly scalable and supports virtual containers. Their storage sub-system is a SAN from Sun Microsystems OEM'ed by Hitachi Data Systems.

They also mandate encryption keys to be safe-guarded at least at FIPS-140-1 level 2.

Challenges

Securing Oracle data files is not an easy task as data files are dynamic, they keep updated at all times which means static way of data encryption offered by encryption utilities are not going to fit the bill.

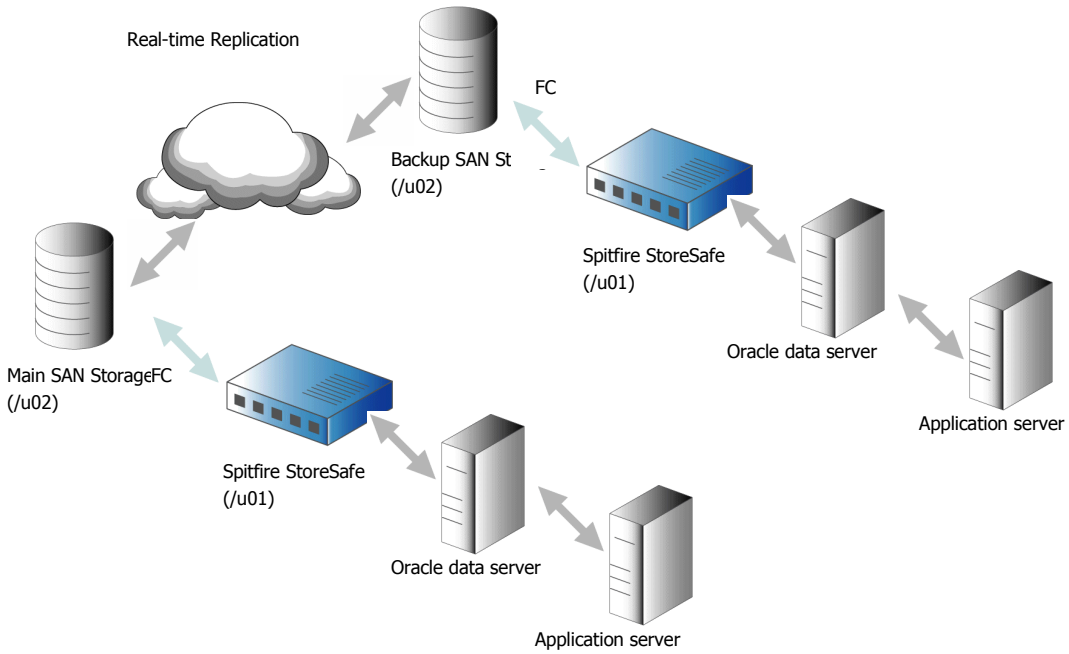
Sensitive data committed to Oracle data files will also be written to database redo logs, archive logs and flash recovery logs. Thus, to secure the system as a whole, all data files, redo, archive and flash recovery logs have to be encrypted.

The Oracle data server runs on a high end system with a very capable SAN storage sub-system, introducing encryption (AES 256-bit as suggested for government use) to the storage path at the same time achieving throughput degradation no more than 30%. It requires a highly multi-threaded, adaptive and scalable encryption solution which can hardly be entertained by ordinary encryption products.

It has to support both the active and standby systems, and guarantees smooth switch-over in worst case scenario.

Solution

To cope with the demanding speed and throughput, Spitfire StoreSafe is installed on the same physical Oracle data server rather than on separate dedicated server. The Oracle data server is scaled up by adding more processors and memory modules to provide enough processing power for both Oracle data server and Spitfire StoreSafe to run without being hunger for system resources.



Configurations

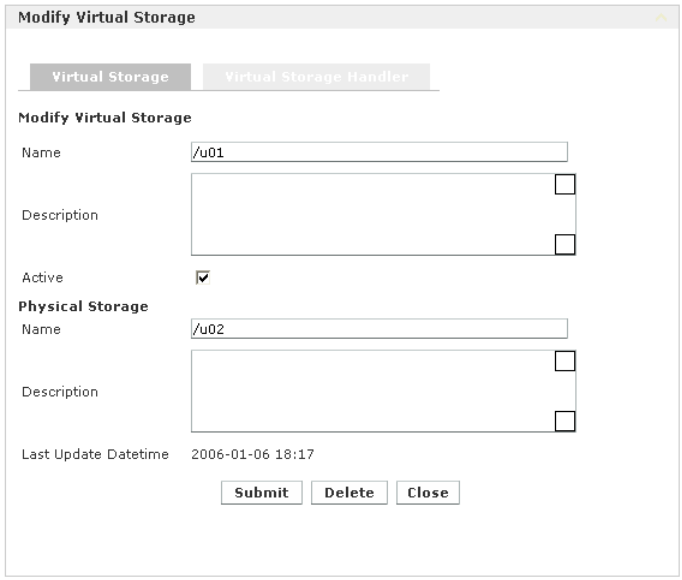
Shutdown Oracle data server.

Assuming Oracle data, redo, archive and flash recovery log files are all located at mount point /u01 of the data server to which the SAN fabric is attached. Backup all files under /u01 follow by clearing all contents. The mount point is detached and remounted as /u02.

Install Spitfire StoreSafe on Solaris platform, and point web browser to https://localhost at data server's GUI console.

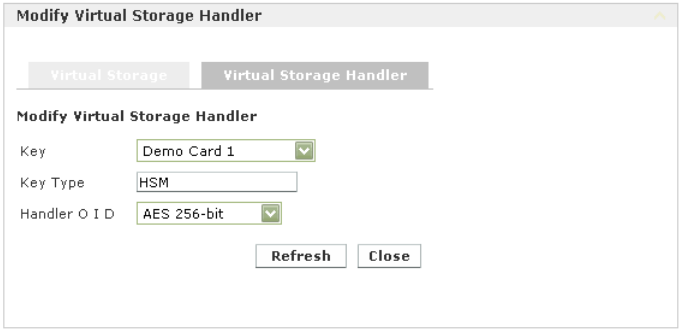
Create new virtual storage as follows

Field	Value
Virtual storage name	/u01
Physical storage	/u02



Turn to Virtual Storage Handler tab, choose Key as 'Demo Card 1' and Encryption algorithm as AES 256-bit

Field	Value
Key	Demo Card 1
Encryption Algorithm	AES 256-bit



Commit and save this new virtual storage configuration. The configurations are backup and restored at the backup site.

Data Migration

Restore backup archive to /u01 at data server. Plain data and log files will get encrypted automatically on-the-fly by Spitfire StoreSafe before they are written to the actual SAN storage at /u02.

Data synchronization mechanism will be able to pick up the changes in form of encrypted data and replicated to the remote site in a timely manner, thus backup replica will assume the same image as soon as data migration is done.

Oracle data server instance is started and application runs seamlessly as before.

Benefits

Data files together with all log files are secured by the same solution. And indeed, Spitfire StoreSafe can be applied on all databases in addition to Oracle.

Migration of database data does not require knowledge of database schemas. For databases with large amount of data at limited cutover time window, one can break down migration into smaller time window and conquer one by one without affecting data integrity and service continuity.

By operating Spitfire StoreSafe with database server, it eliminates performance bottleneck which exists at the connectivity between Spitfire StoreSafe appliance and host servers in standalone deployment scenario. As Spitfire StoreSafe runs on the host which attaches to the storage network directly, it guarantees to be compatible to the storage infrastructure that is hardly attained by other hardware-based solutions.

Spitfire StoreSafe scales with the data server. One can easily cope with increase in throughput demand by adding more processors and main memory.

As encrypted data are written to the storage sub-system, delta changes of files are replicated and sent over the data synchronization network in their encrypted form – additional data security.

Backup and restore operate as before with benefit that backup archives are encrypted by nature.