interopLab

Bloombase StoreSafe Oracle Database Server Encryption on IBM AIX Application Notes

A Quick Guide to Securing Oracle Database Server Data Files on AIX Platform

2007/12/12

Executive Summary

Bloombase StoreSafe storage security server protects privacy of sensitive enterprise data by transparent encryption and decryption. This paper summarizes quick notes to setup of Bloombase StoreSafe and simple migration of Oracle database on IBM AIX platform installed on IBM p-Series POWER based server with IBM DS4100 SAN storage sub-system to achieve transparent Oracle encryption meeting various information security regulatory compliance standards without sacrificing performance.

BLOOMBASE®

Document No.

Table of 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.

This application note discusses the application of Bloombase Spitfire StoreSafe storage security server to protect the most popular enterprise database server in the world, Oracle, where sensitive business information from ERP, knowledge base to

contents, etc are stored, achieving transparent deployment and performance encryption without tedious schema alteration or application change.

Purpose and Scope

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 as well. Bloombase Spitfire StoreSafe storage security server provides a single solution to various information security problems that place huge threats to sensitive data stored in Oracle databases.

This document describes application of Bloombase Spitfire StoreSafe storage security server on Oracle databases installed on IBM AIX operating system to secure sensitive database information at rest transparently without tedious second development efforts and numerous deployment risks and enables customers to protect their private business information and immediately achieve various information security regulatory compliances and standards.

Assumptions

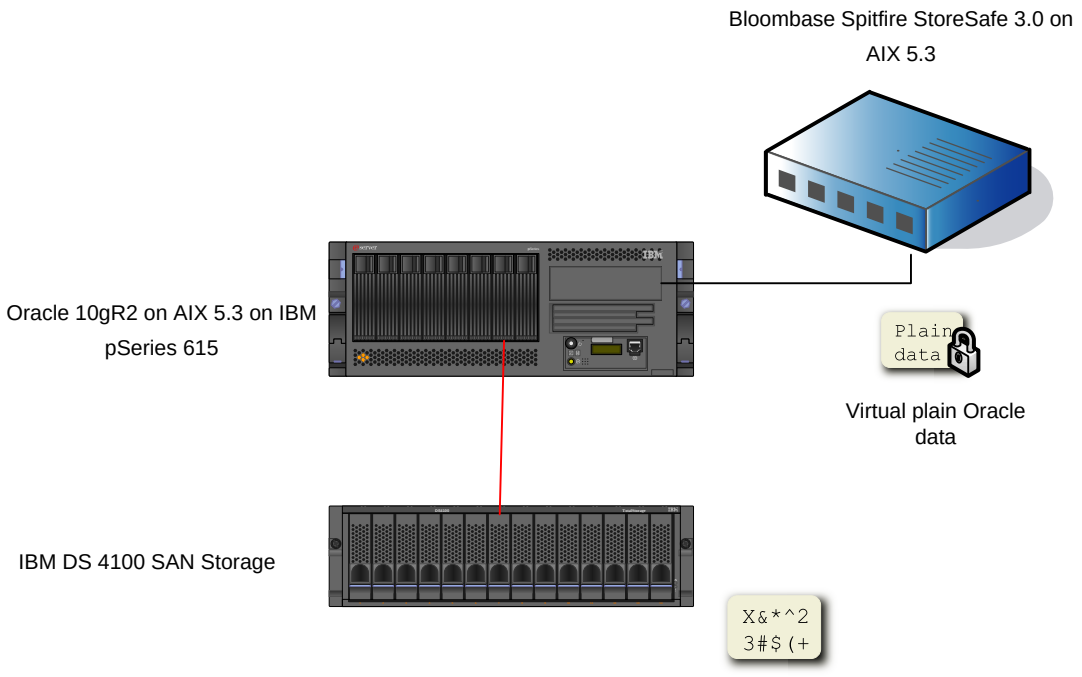
This document describes interoperability testing of Bloombase Spitfire StoreSafe storage security server 3.0 on Oracle 10g release 2 database server on IBM AIX 5.3 ML 4.

We assume you have basic knowledge of administration of Oracle and AIX.

Infrastructure

Setup

The interoperability testing environment is setup as in below figure



Server

Server	IBM pSeries p5 550
Processors	8 x IBM POWER5+ 1.65 Hz
Memory	16 GB
Operating System	IBM AIX 5.3 ML 4

Storage Area Network (SAN)

SAN Storage	IBM DS4100
Link Speed	4 Gbps
Cache Size	2 GB

Software

Oracle	Oracle Databaser Server 10g R2
Spitfire StoreSafe	Bloombase Spitfire StoreSafe storage security server 3.0

Configuration Overview

System Configuration

Virtual Memory

As Bloombase Spitfire StoreSafe is installed on the same physical server and OS instance with Oracle database server sharing the same virtual memory and filesystem cache for both Oracle and Bloombase Spitfire StoreSafe, system virtual memory parameters have to be tuned to avoid exhaust of memory which might lead to unpredictable problems when vast amount of storage data are accessed where Oracle and Spitfire StoreSafe will compete for memory resources

Tune AIX virtual memory parameters as

```
$ vmo -p -o minfree=3840 -o maxfree=4352

$ vmo -p -o maxperm%=40 -o maxclient%=40
```


Spitfire StoreSafe Setup

Spitfire StoreSafe supports both file-based and block-based on-the-fly storage encryption. As a quick start, an Oracle data file is to be secured by Spitfire StoreSafe file-based encryption and will be migrated to Spitfire StoreSafe virtual storage and accessed enabling transparent data encryption and decryption on-the-fly.

Spitfire StoreSafe file-based virtual storage and physical storage settings are configured as followings.

Assume an Oracle database instance named

```
hammer
```

is to be secured by Bloombase Spitfire StoreSafe having its flash recovery area and data file located at filesystem

Repository	Physical Location
Flash recovery area	/u02/flash_recovery_area
Oracle data	/u02/oradata/hammer/

What we want to achieve is to have all files under

```
/u02
```

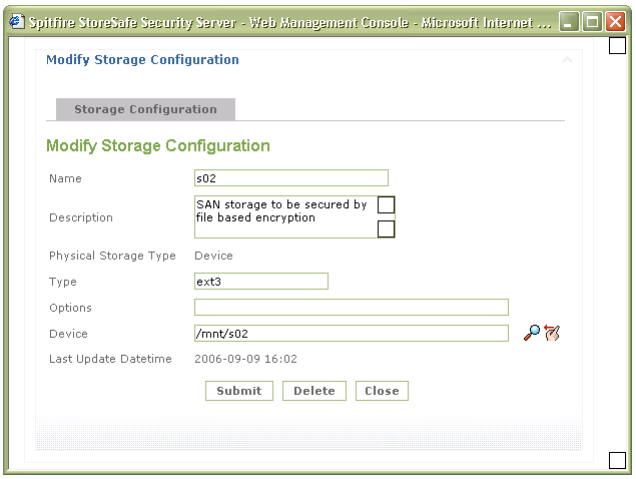
to get secured by Spitfire StoreSafe.

Physical storage u02 is configured in Spitfire StoreSafe server with storage physically located in IBM DS 4100 SAN accessible at filesystem path

/u02

u02 physical storage is configured to run on JFS filesystem as configured via Spitfire StoreSafe web-based management console.

Parameter	Value
Name	hammer_physical
Physical Storage Type	Local
Location	/u02_physical

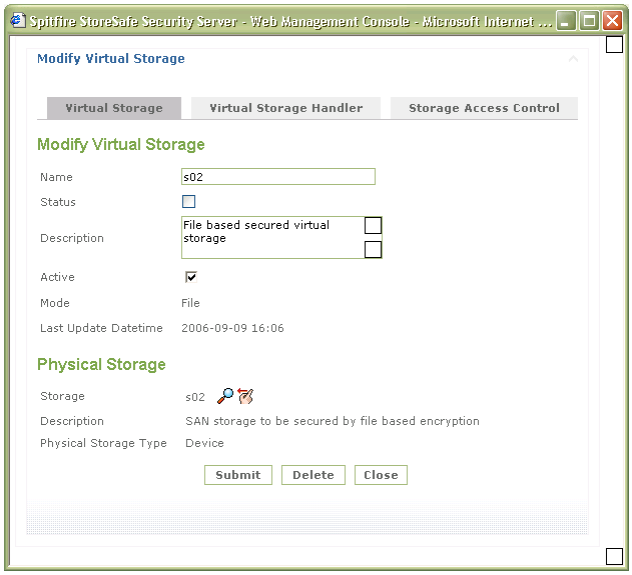


Virtual storage namely hammer is created on Spitfire StoreSafe storage encryption server to virtualize physical SAN storage hammer_physical as a network share. hammer virtual storage is secured using AES 256-bit cryptographic cipher and is configured to be accessible by authorized hosts only using storage networking protocols including NFS.

Plain persistent data are sent from storage host to Spitfire StoreSafe via NFS and/or CIFS. When Spitfire StoreSafe intercepts the plain sensitive contents, they are encrypted on-the-fly and committed to IBM DS 4100 SAN storage.

Parameter	Value
Name	hammer
Mode	File
Physical Storage	hammer_physical
Protection Scheme	Privacy
Key	demo_valid1

Cipher Algorithm	AES
Bit Length	256
Host Security	• 127.0.0.1 • readable and writable



Oracle Database Setup and Migration

Oracle flash recovery area and oradata are now in plain without protection. To secure Oracle data, customers have to follow below steps to migrate and setup filesystem to enable Oracle to access ciphered data AS-IF they are in plain

- Setup Spitfire StoreSafe virtual plain storage
- Migrate Oracle data

IMPORTANT: Make sure Oracle database server is brought to a stop on data migration or serious data corruption might occur. Please make sure you keep a separate database backup for rollback in case of disaster in the middle of migration.

Setup Spitfire StoreSafe Virtual Storage

Plain Oracle data are now stored under

```
/u02
```

and recall last section that Spitfire StoreSafe virtual storage has its physical storage setup at

```
/u02_physical
```

What we need to do is to setup mount point at

```
/u02
```

to enable filesystem read/write actions to route through Spitfire StoreSafe virtual storage

```
hammer
```

so that the sensitive Oracle data contents get transparently encrypted and migrated to physically stored at its pre-configured physical location

Rename current plain Oracle data repository

```
$ mv /u02 /u02_plain
```

Setup mount point /u02 for hammer Spitfire StoreSafe virtual storage

```
$ mount -o hard,llock,rw,bg,timeo=600,wsize=32768,rsize=32768,intr 127.0.0.1:/hammer /u02
```

Automate auto-mount of Spitfire StoreSafe virtual storage by configuring below in

```
/etc/filesystems
```

```
/u02:
        Dev = 127.0.0.1:/hammer
        vfs = nfs
        mount     = false
        options   = rw,bg,timeo=600,hard,llock,wsize=32768,rsize=32768,intr
```

Verify Spitfire StoreSafe virtual storage hammer by creating a test file

```
$ vi /u02/test.txt
```


Browse virtual plain contents of the test file by invoking command in prompt

```
$ cat /u02/test.txt
```

where virtual-plain contents can be seen

Verify encrypted physical file at

/u02_physical/test.txt

by command

```
$ cat / u02_physical/test.txt
```

where contents are physically stored at IBM DS4100 SAN as ciphered and secured.

Migrate Oracle Data Files

Migrate plain Oracle contents to Spitfire StoreSafe virtual storage by

```
$ cp –R /u02_plain/* /u02
```

With above action, database flash recovery area, archive log, redo log, control files, data system files and database user files get encrypted and migrated to the same IBM DS-series SAN disk via Spitfire StoreSafe virtual storage.

Sensitive Data	Location
Flash recovery area	/u02/flash_recovery_area
Redo log	• /u02/hammer/redo01.log • /u02/hammer/redo02.log • /u02/hammer/redo03.log
Database control files	• u02/hammer/control01.ctl • /u02/hammer/control02.ctl

	• /u02/hammer/control03.ctl
Database system files	/u02/hammer/system01.dbf
Database user files	/u02/hammer/users01.dbf
Database temp tablespace files	/u02/hammer/temp01.dbf

Validation Tests

Startup Oracle database instance 'hammer' as normal and issue test SQLs to verify if sensitive data are transparently decrypted on database select whereas they are transparently encrypted on database insert and update

```
$ sqlplus user/password

SQL*Plus: Release 10.2.0.1.0 - Production on Thu Apr 3 06:50:59 2007

Copyright (c) 1982, 2005, Oracle.  All rights reserved.


Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL> select count(*) from CREDIT_CARD;

  COUNT(*)
----------
    500016

SQL>
```

Conclusion

Bloombase Spitfire StoreSafe storage security server protects privacy of sensitive enterprise data by transparent encryption and decryption. This paper summarizes quick notes to setup of Spitfire StoreSafe and simple migration of Oracle database on IBM AIX platform installed on IBM p-Series POWER based server with IBM DS4100 SAN storage sub-system to achieve transparent Oracle encryption meeting various information security regulatory compliance standards without sacrificing performance.

Disclaimer

The tests described in this paper were conducted in the Bloombase InteropLab. Bloombase has not tested this configuration with all the combinations of hardware and software options available. There may be significant differences in your configuration that will change the procedures necessary to accomplish the objectives outlined in this paper. If you find that any of these procedures do not work in your environment, please contact us immediately.

Technical Reference

1. Bloombase Spitfire StoreSafe storage security server certified on IBM Tivoli Storage Manager, eServer xSeries, eServer p5 and IBM DS series SAN storage, http://www-304.ibm.com/jct09002c/gsdod/solutiondetails.do?solution=27715

2. Oracle Storage Program Change Notice, http://www.oracle.com/technology/deploy/availability/htdocs/oscp.html

3. Oracle Database Protection by Spitfire StoreSafe, http://www.bloombase.com/download/index.jsp?Url=/products/spitfire/storesafe/OracleDatabaseProtectionBySpitfireStoreSafe.pdf

4. Spitfire StoreSafe Compatibility Matrix, http://www.bloombase.com/download/index.jsp?Url=/products/spitfire/storesafe/SpitfireStoreSafeNASCompatibilityMatrix.pdf