

interopLab

Bloombase StoreSafe and Oracle Database Server on IBM HACMP Application Notes

A Quick Guide to Deploy Bloombase StoreSafe on an IBM HACMP Cluster with Oracle Database

2008/02/28

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 in High Availability environment on IBM AIX platform installed on IBM p-Series POWER based server with the HACMP software and IBM DS4100 SAN storage sub-system to achieve transparent Oracle encryption meeting various information security regulatory compliance standards without sacrificing performance.

BLOOMBASE®

IBM System Storage Proven™

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.

Bloombase Spitfire StoreSafe also offers option for High Availability scenario in IBM AIX operation system with the utilization of High Availability Cluster Multi-Processing (HACMP).

Assumptions

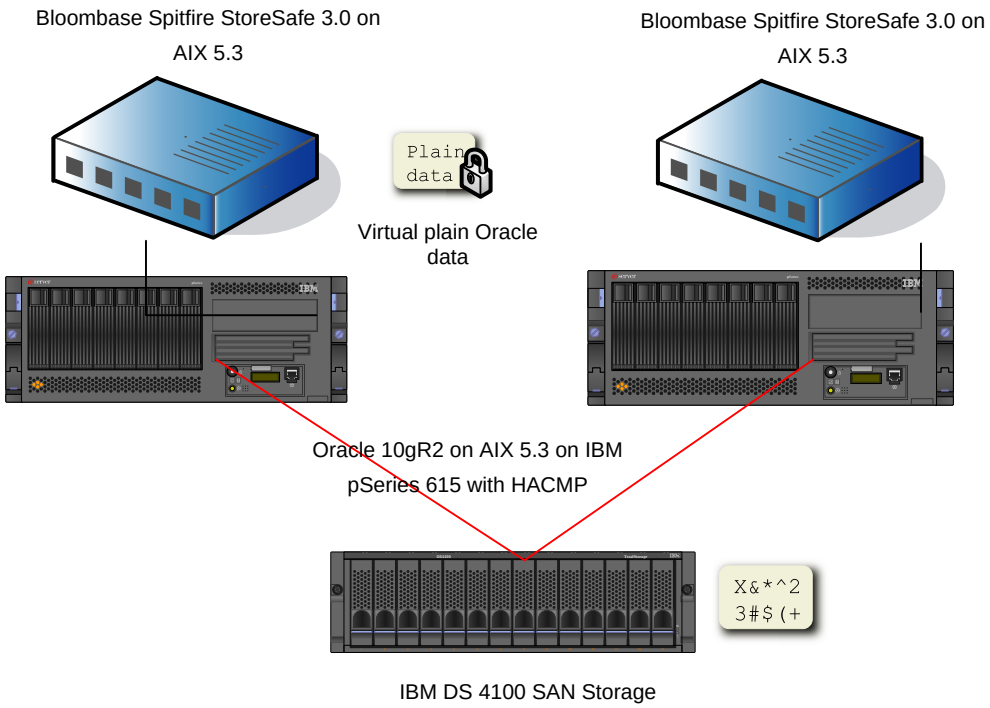
This document describes interoperability testing of Bloombase Spitfire StoreSafe storage security server 3.0 on Oracle 10g release 2 database server on IBM AIX 5.3 ML 4, with HACMP 5.3

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

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

HACMP	IBM AIX HACMP 5.3
Oracle	Oracle Databaser Server 10g R2
Spitfire StoreSafe	Bloombase Spitfire StoreSafe storage security server 3.0

Configuration Overview

Before we start, assume the HACMP cluster consists of 2 nodes :

```
node1
```

```
node2
```

where node1 is the active node.

And Oracle database server is existing as an application server

```
orainstance
```

which is contained in the cluster resource group

```
orainstance
```

Spitfire StoreSafe is installed on both the cluster nodes at

```
/spitfire
```


HACMP Setup

High availability is ensured for Spitfire StoreSafe in an HACMP cluster. In case of a system failure, under HACMP control, Spitfire StoreSafe is moved to another node in the cluster. System Management Interface Tool (SMIT) is used for the HACMP configuration.

Preparation

Before we setup HACMP configuration for Spitfire StoreSafe, we need to perform :

1 Shutdown the cluster service at both nodes, which will shutdown the oracle application server as well

2 Unmount the virtual storage mount point

3 Stop Spitfire StoreSafe.

4 Enable system to startup Spitfire StoreSafe in standby mode in both nodes :

4.1 Enable Spitfire StoreSafe to startup during system startup

```
$ ln -s /usr/bin/storesafe /etc/rc.d/rc2.d/Sstoresafe
$ ln -s /usr/bin/storesafe /etc/rc.d/rc2.d/Kstoresafe
```

4.2 Change the default startup mode of Spitfire StoreSafe in both nodes, modify the Registry through Spitfire StoreSafe Management Console :

```
System > SpitfireApplication > DefaultStatus = 0
```


Create Application Server for Spitfire StoreSafe

By HACMP, we first add an Application Server for Spitfire StoreSafe.

```
$ smit hacmp
```

Select the following menu items :

```
Extended Configuration

Extended Resources Configuration

HACMP Extended Resources Configuration

Configure HACMP Applications

Configure HACMP Application Servers

Add an Application Server
```

Enter the fields as follows :

Parameter	Value
Server Name	storesafe
Start Script	/spitfire/storesafe/WEB-INF/scripts/aix/spitfiremodule startup
Stop Script	/spitfire/storesafe/WEB-INF/scripts/aix/spitfiremodule standby

Create Resource Group for Spitfire StoreSafe

We then add a Resource Group for Spitfire StoreSafe.

```
$ smit hacmp
```

Select the following menu items :

```
Extended Configuration

Extended Resources Configuration

HACMP Extended Resource Group Configuration

Add a Resource Group
```

Enter the fields as follows :

Parameter	Value
Resource Group Name	storesafe
Participating Nodes	node1 node2
Startup Policy	Online On First Available Node
Fallover Policy	Fallover To Next Priority Node In The List
Fallback Policy	Never Fallback

Add Application to the Resource Group for Spitfire StoreSafe

We then add the application to the Resource Group for Spitfire StoreSafe.

```
$ smit hacmp
```

Select the following menu items :

```
Extended Configuration

Extended Resources Configuration

HACMP Extended Resource Group Configuration

Change/Show Resources and Attributes for a Resource Group
```

Select the Resource Group `storesafe`

Enter the fields as follows :

Parameter	Value
Application Servers	storesafe

By the above configuration, starting the resource group

```
storesafe
```

will start the application server

```
storesafe
```


Create Application Server for Virtual Storage Mount

Setup 2 shell scripts mount.sh and umount.sh on both cluster nodes :

where mount.sh is is to setup mount point /u02 for hammer Spitfire StoreSafe virtual storage hammer

```
#! /bin/sh
/etc/mount -o hard,llock,rw,bg,timeo=600,wsize=32768,rsize=32768,intr 127.0.0.1:/hammer /u02
```

umount.sh is is to unmount the mount point

```
#! /bin/sh
/etc/umount /u02
```

With these scripts, we can proceed to add an Application Server for Spitfire StoreSafe Virtual Storage Mount.

```
$ smit hacmp
```

Select the following menu items :

```
Extended Configuration

Extended Resources Configuration

HACMP Extended Resources Configuration

Configure HACMP Applications

Configure HACMP Application Servers

Add an Application Server
```

Enter the fields as follows :

Parameter	Value
Server Name	Vsmount
Start Script	/scripts/vsmount/mount.sh
Stop Script	/scripts/vsmount/umount.sh

Create Resource Group for Virtual Storage Mount

We then add a Resource Group for Spitfire StoreSafe Virtual Storage Mount.

```
$ smit hacmp
```

Select the following menu items :

```
Extended Configuration

Extended Resources Configuration

HACMP Extended Resource Group Configuration

Add a Resource Group
```

Enter the fields as follows :

Parameter	Value
Resource Group Name	vsmount
Participating Nodes	node1 node2
Startup Policy	Online On First Available Node
Fallover Policy	Fallover To Next Priority Node In The List
Fallback Policy	Never Fallback

Add Application to the Resource Group for Virtual Storage Mount

We then add the application to the Resource Group for Spitfire StoreSafe Virtual Storage Mount.

```
$ smit hacmp
```

Select the following menu items :

```
Extended Configuration

Extended Resources Configuration

HACMP Extended Resource Group Configuration

Change/Show Resources and Attributes for a Resource Group
```

Select the Resource Group `vsmount`

Enter the fields as follows :

Parameter	Value
Application Servers	vsmount

By the above configuration, starting the resource group

`vsmount`

will start the application server

`vsmount`

Create Dependency for the resource groups

To maintain the application execution order, we will create resource groups dependency so that Spitfire StoreSafe is run first, then Virtual Storage Mount, and oracle instance the last one.

```
$ smit hacmp
```

Select the following menu items :

```
Extended Configuration

Extended Resource Configuration

Configure Resource Group Run-Time Policies

Configure Dependencies between Resource Groups

Configure Parent/Child Dependency

Add Parent/Child Dependency between Resource Groups
```

Select

```
storesafe
```

as the Parent Resource Group and select

```
vsmount
```

as the Child Resource Group

The parent/child dependency is therefore established for the resource groups

```
storesafe/vsmount
```

Repeat these steps to establish parent/child dependency for the resource groups

```
vsmount/orainstance
```


Create Location Dependency

Since Spitifre StoreSafe, Virtual Storage Mount and Oracle instance all need to run on the same node, the Same Node Dependency provide the convenience :

```
$ smit hacmp
```

Select the following menu items :

```
Extended Configuration

Extended Resource Configuration

Configure Resource Group Run-Time Policies

Configure Dependencies between Resource Groups

Configure Online on the Same Node Dependency

Add Online on the Same Node Dependency Between Resource Groups
```

Enter the fields as follows :

Parameter	Value
Resource Groups to be Online on the same node	storesafe vsmount orainstance

Create Application Monitor

We suggest to setup an application monitor on the Spitfire StoreSafe virtual storage, in order to ensure the virtual storage NFS share is created before the mount point is established

```
$ smit hacmp
```

Select the following menu items :

```
Extended Configuration

Extended Resource Configuration

HACMP Extended Resources Configuration

Configure HACMP Applications

Configure HACMP Application Monitoring

Configure Custom Application Monitors

Add a Custom Application Monitor
```

Enter the fields as follows :

Parameter	Value
Monitor Name	checkmount
Application Server to Monitor	storesafe
Monitor Mode	Startup Monitoring
Monitor Method	/scripts/vsmount/checkmount.sh
Stabilization Interval	120
Restart Count	0
Action on Application Failure	fallover

This means the application monitor checks the Spitfire StoreSafe virtual storage NFS share creation within the stabilization interval. If the virtual storage mount is created successfully, it proceeds to the next resource group, ie `vsmount`.

Here is the checkmount.sh :


```
#! /bin/sh
SHARE_FOUND=`showmount -e localhost | grep "/hammer"`
if [ "$SHARE_FOUND" = "" ]
then
   exit 1
else
   exit 0
fi
```

Verify and Synchronize the cluster

After all the above resource groups, dependencies and monitors are setup, we need to synchronize so that all nodes in the cluster have the same configuration

```
$ smit hacmp
```

Select the following menu items :

```
  Initialization and Standard Configuration

  Verify and Synchronize HACMP Configuration
```


Validation Tests

Restart both nodes so that Spitfire StoreSafe is in standby mode in both nodes. With the cluster running in both nodes, after a while, the cluster status should show that the application servers are running at node1:

```
            clstat - HACMP Cluster Status Monitor
            -------------------------------------

Cluster: bloombase     (1206514934)
Fri Nov 23 16:40:01 GMT 2007
            State: UP            Nodes: 2
            SubState: STABLE


      Node: node1          State: UP
        Interface: node1 (0)            Address: 172.23.136.8
                                        State:   UP
        Interface: node1_tty0 (1)          Address: 0.0.0.0
                                        State:   UP
        Interface: node1_srv (0)         Address: 172.23.138.200
                                        State:   UP
        Resource Group: orainstance               State:  On line
        Resource Group: storesafe                   State:  On line
        Resource Group: vsmount                    State:  On line

      Node: node2          State: UP
        Interface: node1 (0)            Address: 172.23.136.9
                                        State:   UP
        Interface: node2_tty0 (1)          Address: 0.0.0.0
                                        State:   UP
```


Oracle database instance ‘hammer’ is therefore started. We can 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. High Aailability of Spitfire StoreSafe is also illustrated with the HACMP tool.

Acknowledgement

We would like to thank the following individuals for their contribution (in terms of consultancy and facilities management) to the testing process and technical report :

Sashikala Rajalingam, IBM Innovation Center

Catharine GH Tan, IBM Innovation Center

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

5. HACMP Administration Guide, http://publib.boulder.ibm.com/epubs/pdf/c2348628.pdf

6. Spitfire StoreSafe Oracle Database Server Encryption on IBM AIX Application Notes, http://www.bloombase.com/download/index.jsp?Url=/products/spitfire/storesafe/SpitfireStoreSafeAIXOracleEncryptionApplicationNotes.pdf