interopLab

Interoperability of Spitfire StoreSafe and Oracle RAC for Transparent Oracle Database Encryption

November 15, 2006

Bloombase®
Least Invasive Security

Executive Summary

Government agencies and financial institutes are mandated by national legislation and/or industry-wide information security standards to have their sensitive storage data secured from prying eyes, otherwise organizations and business owners are liable to prosecution, fines or contract annulment if sensitive customer data are ever exposed. Oracle Database is the de-facto standard in the industry for relational data management whereas Real Application Cluster (RAC) is specifically designed for mission critical non-stop systems where data service availability is of the highest requirements. Bloombase's Spitfire StoreSafe application transparent enterprise storage encryption server is validated to run with Oracle 10g RAC on Sun Solaris operating system. This document describes the steps carried out to test interoperability of Oracle 10g RAC and Spitfire StoreSafe in Oracle Competency Center.

Document No.

This interoperability test is sponsored by Oracle Corporation and took place at Shenzhen Software Park Oracle Compentency Center (SSPOCC)
http://www.oracle.com/cdc/sspocc/index.html

For more information on this interoperability test, please contact

Table of Contents

Purpose and Scope

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 document describes the steps necessary to integrate Spitfire StoreSafe enterprise storage security server with Oracle 10g RAC to secure sensitive corporate business data in a storage. Specifically, we cover the following topics:

- Configuration of Oracle RAC
- Installation and configuration Spitfire StoreSafe server
- Filesystem and Oracle interoperability testing

Assumptions

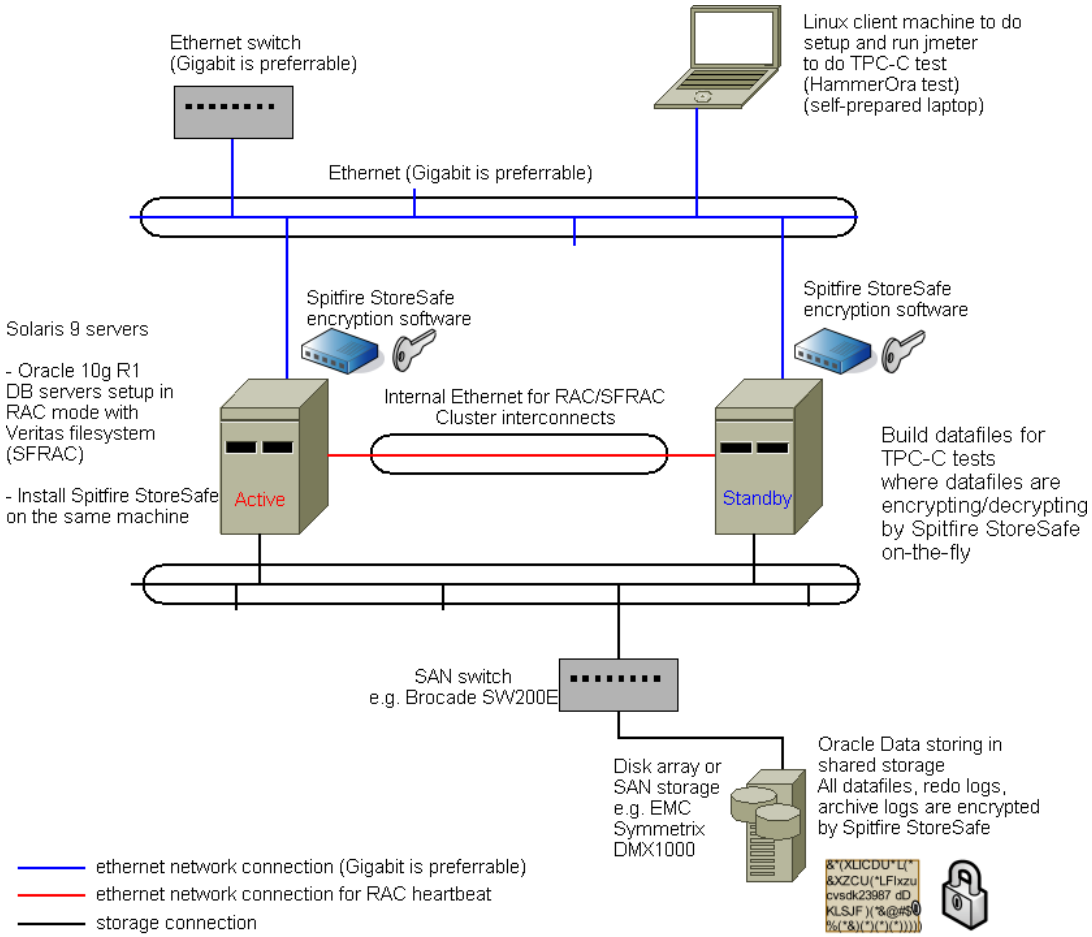
This document describes interoperability testing of Spitfire StoreSafe server with Oracle RAC . Therefore, it is assumed that you are familiar with operation of Oracle, storage systems and Solaris operating system. It is also assumed that you posssess basic UNIX administration skills. The examples provided may require modifications before they are run under your version of UNIX.

You are recommended to refer to installation and configuration guides of Oracle RAC for the platform you are going to test on. We assume you have basic knowledge of storage networking and information cryptography. For specific technical product information of Spitfire StoreSafe, please refer to our website at http://www.bloombase.com or Bloombase SupPortal http://supportal.bloombase.com

Infrastructure

Setup

The validation testing environment is setup as in below figure



- Spitfire StoreSafe for Solaris software is installed onto each node of the Oracle RAC cluster
- Virtual storage is created and configured on Spitfire StoreSafe to physically access shared storage in SAN
- Say for instance confidential data are required to be persisted at /rac_ts/oradata/hamvx, an encrypted virtual storage is created at Spitfire StoreSafe's management console at /rac_ts/oradata/hamvx_safe as a storage gateway to /rac_ts/oradata/hamvx
- Confidential Oracle data, redo, archive log files read/write via encrypted virtual storage triggers Spitfire StoreSafe to encrypt and decrypt storage data realtime on-the-fly according to the cryptographic configurations preset in Spitfire StoreSafe including cipher algorithms, encryption keys, additional access control and key length, etc
- Confidential data in form of files are encrypted by Spitfire StoreSafe software with a fixed header size of 8KB
- Spitfire StoreSafe software integrates with operating system and applications (Oracle) seamlessly by creating virtual storage on the system allowing application's access transparency
- Spitfire StoreSafe runtime shares the hardware resources (processor, memory, etc) of the database servers, no additional hardware purchase is required
- Upgrade of database hardware automatically scales up Spitfire StoreSafe for greater cryptographic processing throughput requirements

Oracle RAC Node

Server	Sun Microsystems SunFire V40z

Processors	2 x AMD Opteron(tm) Processor 848 2.2GHz
Memory	3.5 GB
Operating System	Oracle Unbreakable Linux (Enterprise Linux Enterprise Linux Server release 4 update 4, kernel 2.6.9-42.0.0.0.1.ELsmp)
Oracle	Oracle 10gR2 RAC

Spitfire StoreSafe Server

Model	Spitfire StoreSafe for Linux version 2.0
Key Management	Built-in Spitfire KeyCastle key management server

Configuration Overview

Storage

A virtual disk is created at StorEdge 3310 with below parameters

Name	ocfs2
Capacity	100 GB
Redundancy	RAID5

Oracle RAC

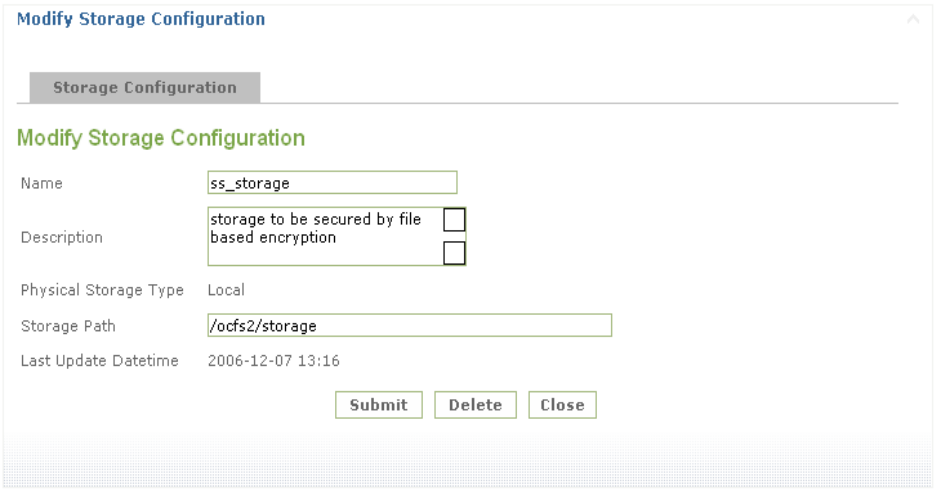
Oracle 10g Release 2

Spitfire StoreSafe

Spitfire StoreSafe supports both file-based and block-based on-the-fly storage encryption. In this interoperability test exercise, file-based encryption mode is validated against Oracle 10g RAC. Spitfire StoreSafe file and block-based virtual storage and physical storage settings are configured as followings.

Physical storage storage is configured in Spitfire StoreSafe for NAS server with storage physically located in SAN storage accessible at path /ocfs2/storage.

Storage physical volume is configured to run on local as shown in below screen capture of Spitfire StoreSafe web-based management console.



Virtual storage namely ss_storage is created on Spitfire StoreSafe for NAS storage encryption server to virtualize physical SAN storage ss_storage as a network share. ss_storage 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 and CIFS.

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

More About Spitfire StoreSafe

Confidential and private information stored in database are sensitive information which are required to be secured according to and governed by various personal data privacy regulatory standards

Without protection, confidential personal data and transaction information stored in Immigration's database systems risk the following data vulnerabilities:-

- Electronic theft by administrators and operators at primary/secondary sites
- Hardware theft (storage sub-systems and hard-drive) at primary/secondary sites
- Eavesdropping and digital disclosure of plain sensitive information via the replication path
- Backup archive and backup media theft

Data Encryption

While perimeter and access control measures block outsiders' attacks, researches have revealed there is a growing trend of insiders' attacks and core/unknown intrusions at the data which expose business/customer privacy and in worst cases, might lead to service discontinuity and business shutdown.

To be able to meet various regional, national and industry information security standards, sensitive customer data and confidential monetary information stored in Immigration's primary/resilience storage sub-systems and backup media should be secured by data encryption.

Data cryptography is the process of turning sensitive plain information into scrambled data which appear to be like garbage by use of a secure cryptographic cipher and user encryption key. Confidential data hidden by encryption are difficult, if not impossible, to be revealed without knowledge of the encryption key. The strength of encryption varies per cipher algorithms and key length. According to NIST, sensitive data archives of government agencies and large enterprises are recommended to be secured by AES 256-bit.

Key Management

As in most large enterprises, sensitive corporate information of different natures might be secured by keys owned by two independent entities of a corporation. Confidential data encrypted by one key over a period of time might need to be re-encrypted by a new key for higher level of security concern.

There is no exception to Immigration Department. They require key management tools easily accessible by users with no or elementary training and be operable by least technical staff within an enterprise, such as CSO or security officers of individual user departments.

Strength of encryption is as strongest and at the same time as weakest as the key by which the sensitive information are protected. For maximum security concerns, there should be options to have keys be stored and secured ONLY in hardware security modules including PKCS#11 HSM appliances, tokens or smartcards.

Platform Independence and Portability

A platform independent and scalable data encryption solution built upon mature storage networking communications protocols is what enterprises require, such that the enterprise system and storage encryption infrastructures can be scaled and extended independently with least hindrance to one another.

The encryption solution should support all major OS including Sun Solaris, HPUX, IBM AIX, Microsoft Windows, Linux, MacOS, etc and all enterprise storage sub-systems no matter they are DAS, NAS or SAN. Bloombase partners with the world leading technology leaders including Sun, EMC, Brocade, Oracle, SNIA, IBM, HP, Redhat, SGI, Novell, AMD and Intel to deliver well-tested and well-tuned solutions supporting all platforms at best performance.

Piecemeal encryption utilities such as Windows EFS, Linux loopback and those exclusively for laptop computers should be avoided and only those designed for enterprise storage systems to be considered.

Ease of Deployment

Customers already have their enterprise system in production. Mission critical systems can only allow transparent of deployment of data encryption without affecting current application and storage infrastructure. Initial data migration should be done and verified by command-and-conquer and be able to breakdown the whole migration volume into smaller manageable pieces such that the 24x7 service is not entirely interrupted.

The encryption solution should be composed of independent hardware appliance modules without the need to sharing database servers' resources in resource intensive cryptographic processing which might introduce resource overheads, congestions and possibly degrade platform stability and efficiency.

High Availability and Disaster Recovery

Enterprise information infrastructure is built on high-availability (HA) architecture. By introducing data encryption into the system, one baseline requirement one can never sacrifice is again, service availability. The data encryption solution should be able to fit in the highly available architecture of the system – data replication and server clustering.

The data encryption solution itself should also be HA-ready as well and be able to operate in redundancies to avoid single point of failure in the ensemble data system.

The encryption solution should be designed and operate at the storage device communications layer such that clustering and high availability software and utilities can ride on top of.

Scalability and Extensibility

The encryption solution should be able to cope with the growing volume of data and data throughput by means of hardware options upgrade or clustering.

Encryption technologies advance year-by-year, if not day-by-day. The ability of cryptographic module upgrade is what Immigration Department is looking for such that by investing in a single solution, they possess the storage security platform meeting their growing security requirements.

Benefits

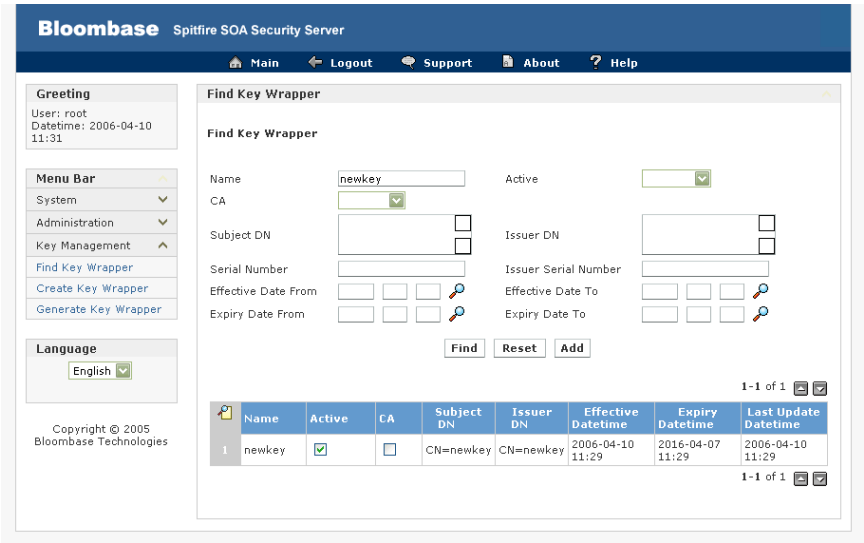
Least Invasive Security

- Files containing sensitive contents are encrypted and secured by strong encryption as persisted in their natural form on the persistence storage sub-system
- Electronic backup archives and physical backup media made on the physical storage are secured by strong encryption
- Complete application transparency
- No application change
- Complete user transparency
- No application client needs to be installed on host thus no user training and least total cost of ownership (TCO)
- Storage contents get encrypted and decrypted by Spitfire StoreSafe under the covers
- Spitfire StoreSafe can integrate with FIPS-140-1 level 2 certified hardware security module for maximum cryptographic key protection
- Cryptographic ciphers include
    - FIPS-197 AES 256-bit, 192-bit, 128-bit
    - FIPS-46-3 3DES and DES
    - Camellia
- Hardware and non-hardware key up to 2048-bit long
- For details technical specifications, please visit: http://www.bloombase.com/products/spitfire/storesafe/specifications.html

Key Management

- Spitfire StoreSafe can work with
    - bundled Spitfire KeyCastle
    - standalone Spitfire KeyCastle appliance
    - hardware security module
- Spitfire StoreSafe key management has the following features

- Centralized web-based key management



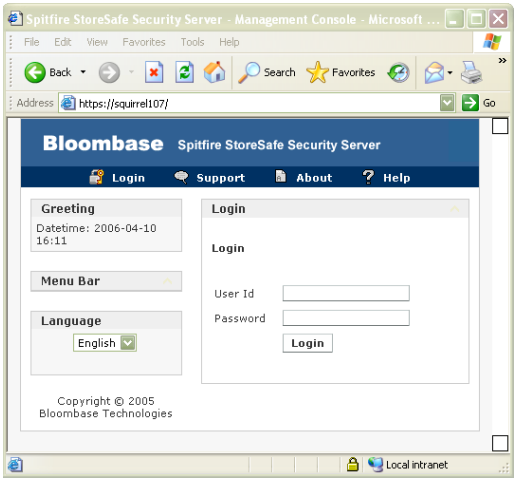
- User friendly web-based management console
- X.509 v3 RSA key generation of lengths 512, 1024 and 2048 bits
- PKCS#12 DER and PEM key storage file import
- KeyCastle key storage protected by PKCS-5 Password-based encryption and NIST-197 AES-256-bit encryption
- PKCS#11 HSM accessibility and secure-socket layer (SSL) channel protection
- VISA Technology level 3 and NIST FIPS-140-2 tamper-proof HSM key storage
- 128, 192 and 256-bit NIST-197 AES key generation
- 56 and 112 bit NIST 46 3DES key generation
- Key activation, deletion and lookup

Manageability

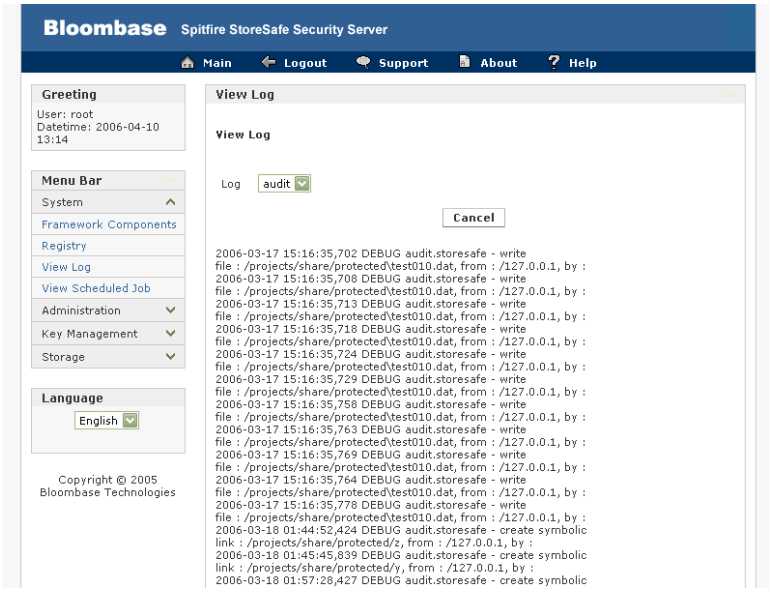
- RS-232 Serial console management

```
<Restart / Shutdown>

1) Restart
2) Shutdown

b) Back to Main Menu

Select : _
```


- HTTPS-secured Web-based management console



- Audit trail



- SNMP and heartbeat

Validation Tests

Test Scenarios

Filesystem Tests

The following tests are carried out at storage hosts to access encrypted SAN storage secured by Spitfire StoreSafe server

Test	Description
Directory creation	Platform equivalence of UNIX's mkdir
Directory rename	Platform equivalence of UNIX's mv
Directory removal	Platform equivalence of UNIX's rm
Directory move	Platform equivalence of UNIX's mv
File creation	Platform equivalence of UNIX's echo XXX >
File rename	Platform equivalence of UNIX's mv
File removal	Platform equivalence of UNIX's rm
File move	Platform equivalence of UNIX's mv
File append – by character	Platform equivalence of UNIX's echo XXX >>
File append – by block	Platform equivalence of UNIX's echo XXX >>
File parameters inquiry	Platform equivalence of UNIX's ls *X

Softlink/Symbolic link removal	• Platform equivalence of UNIX's rm • Valid for UNIX-based storage host systems only (Linux, AIX, HPUX, Solaris)
Softlink/Symbolic link move	• Platform equivalence of UNIX's mv • Valid for UNIX-based storage host systems only (Linux, AIX, HPUX, Solaris)

Oracle Database Test

Test	Remarks
Database creation	Version equivalence of CREATE DATABASE
Schema creation	Version equivalence of CREATE USER
Table creation	Version equivalence of CREATE TABLE
Database record insert	Version equivalence of INSERT INTO
Database record query	Version equivalence of SELECT * FROM
Database record update	Version equivalence of UPDATE
Database record delete	Version equivalence of DELETE FROM
Index creation	Version equivalence of CREATE INDEX
Tablespace alteration	Version equivalence of ALTER TABLESPACE
Redo log creation	Automated by Oracle data server, verify by examining Oracle system log
Redo log rotation	Automated by Oracle data server, verify by examining Oracle system log
Archive log creation	Automated by Oracle data server, verify by examining Oracle system log

Oracle Database Access Test

Test	Remarks
TPCC query tests	queries

Oracle RAC Test

Test	Remarks
Database instance starts and joins cluster	
Instance failover	Active node network interface inactivated
Database shutdown	
Database creation	
Table creation	
Index creation	

Record insert	
Record select	
Record update	
Record delete	

Result

Filesystem Tests

Test	Validation Pass	Remarks
Directory creation (Under directory /ocfs2/storage)	✓✓	mkdir test
Directory rename	✓✓	mv test sstest
Directory move	✓✓	mv sstest ../
Directory removal	✓✓	rm -r sstest
File creation	✓✓	vi abc.txt
File rename	✓✓	mv abc.txt qwert.txt
File move	✓✓	mv qwert.txt oradata/
File removal	✓✓	rm oradata/qwert.txt
File append – by character	✓✓	echo "good evening" >>abc.txt
File append – by block	✓✓	cat >> abc.txt << eof
		good
		eof
File parameters inquiry	✓✓	ls -al
Softlink/Symbolic link removal	✓	ln -s /ocfs2/bloombase/ /ocfs2/virtual_storage/
Softlink/Symbolic link move	✓	mv /ocfs2/bloombase flash_recovery_area/

Oracle Database Test

Test	Validation Pass	Remarks
Database creation	✓	Setup new database instance through issue 'dbca'.
Schema creation	✓	create user orabm identified by orabm tempoary tablespace temp;
		alter user orabm default tablespace users;
		alter user orabm quota unlimited on users;

Table creation	✓	create table orabm.contents (title varchar2(1024) null, link varchar2(1024) null, description clob null, last_upd_dt timestamp null);
Database record insert	✓	insert into orabm.contents values (“abc”, “abc”, “abc”, 0);
Database record query	✓	select * from orabm.contents;
Database record update	✓	update orabm.contents set title=”efg” where title=”abc”;
Database record delete	✓	delete from orabm.contents where title=”efg”;
Index creation	✓	create index contentsi2 on contents (last_upd_dt);
Tablespace alteration	✓	alter tablespace temp add tempfile '/oradata/apple/temp01.dbf' size 36m;
Redo log creation	✓	alter database add logfile ('/ocfs2/oradata/sspocc/redo04.log') size 10m;
Redo log rotation	✓	alter system switch logfile;
Archive log creation	✓	alter database archivelog;

Oracle Database Access Test

Test	Validation Pass	Remarks
TPCC query tests	✓✓	Test through jmeter

Oracle RAC Test

Test	Validation Pass	Remarks
Database instance starts and joins cluster	✓	Setup new database instance through issue 'dbca'. A warning shows “Directory /ocfs2/oradata/sspocc is not on the cluster filesystem shared by rac1, rac2” before move to next step. It disappeared after several trials when click on “next”.
Instance failover	✓	ifconfig eth0 down can get correct results of query
Database shutdown	✓	Sqlplus / as sysdba SQL> shutdown
Database creation	✓	Setup new database instance through issue 'dbca'.
Table creation	✓	create table orabm.contents (title varchar2(1024) null, link varchar2(1024) null, description clob null, last_upd_dt timestamp null);
Index creation	✓	insert into orabm.contents values (“abc”, “abc”, “abc”, 0);
Record insert	✓	insert into orabm.contents values (“abc”, “abc”, “abc”, 0);
Record select	✓	select * from orabm.contents;
Record update	✓	update orabm.contents set title=”efg” where title=”abc”;

Record delete	✓	delete from orabm.contents where title=”efg”;

Conclusion

All test scripts are executed and returned without errors. Oracle RAC passes all Bloombase interopLab's interoperability tests with Spitfire StoreSafe enterprise storage encryption server

Bloombase Product	Operating System	Third Party Products
Spitfire StoreSafe	Oracle Unbreakable Linux	• Oracle 10g RAC