



Interoperability of Bloombase StoreSafe Security Server, QLogic FC-HBAs and QLogic SAN Switch for Transparent Storage Area Network (SAN) Encryption

December, 2012

BLOOMBASE[®]



Executive Summary

QLogic enterprise grade fiber channel host bus adapters (FC-HBA) and SAN switches are validated by Bloombase's interopLab to run with Bloombase StoreSafe application-transparent storage area network (SAN) encryption server. This document describes the steps carried out to test interoperability of QLogic Fiber Channel HBAs and SAN switches with Bloombase StoreSafe Storage Encryption Server on SpitfireOS running on x86-based appliances. Host systems on Microsoft Windows, Linux, Solaris, IBM AIX, VMware and Citrix XenServer are validated against QLogic-powered Bloombase StoreSafe Storage Encryption appliances with Dell EMC SAN storage sub-system. Host software applications including Oracle Database and Symantec Veritas Storage Foundation for Oracle Real Application Cluster (SFRAC) are also validated.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, people and events depicted herein are fictitious and no association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Bloombase.

Bloombase may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Bloombase, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

This document is the property of Bloombase. No exploitation or transfer of any information contained herein is permitted in the absence of an agreement with Bloombase, and neither the document nor any such information may be released without the written consent of Bloombase.

© 2012 Bloombase, Inc.

Bloombase, Spitfire, Keyparc, StoreSafe are either registered trademarks or trademarks of Bloombase in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Document No.

Table of Contents

Table of Contents	3
Purpose and Scope	5
Assumptions	6
Infrastructure	7
Setup	7
Bloombase StoreSafe Storage Encryption Server Appliance	8
Fiber Channel Host Bus Adapters	8
SAN Switch	9
Storage Area Network (SAN)	9
Storage Hosts	9
Optical Fiber Cables	9
Configuration Overview	10
QLogic FC-HBA	10
SAN Fabric	11
SAN Storage	14
Optical Fiber Cables	14
Bloombase StoreSafe Security Server	15
Encryption Key Configuration	15

Virtual SAN Configuration	16
Physical Storage Target Configuration	17
Encrypted Virtual Storage Provisioning	18
Validation Tests	20
Test Scenarios	20
Validation Matrix	20
Raw Storage Device Tests	21
File System Tests	22
Application Tests – Oracle Database Server on Symantec Veritas Storage Foundation for Oracle RAC	23
Result	23
Raw Storage Device Tests	23
File System Tests	24
Application Tests – Oracle Database Server on Symantec Veritas Storage Foundation for Oracle RAC	24
Conclusion	26
Acknowledgement	28
Disclaimer	29
Technical Reference	30

Purpose and Scope

This document describes the steps necessary to integrate QLogic FC-HBAs and SAN switches with Bloombase StoreSafe enterprise storage security server to secure sensitive corporate business data in a storage area network (SAN). Specifically, we cover the following topics:

- Preparing Bloombase StoreSafe Security appliance(s) with QLogic FC-HBA(s)
- Preparing QLogic Sanbox 5800V Fabric SAN Switch
- Preparing SAN storage sub-system
- Interoperability testing on host systems including Red Hat Linux, Novell Linux, Microsoft Windows, IBM AIX, Solaris, VMware ESX and Citrix XenServer
- Interoperability testing with Oracle Database and Symantec Storage Foundation for Real Application Cluster (SF-RAC)

Assumptions

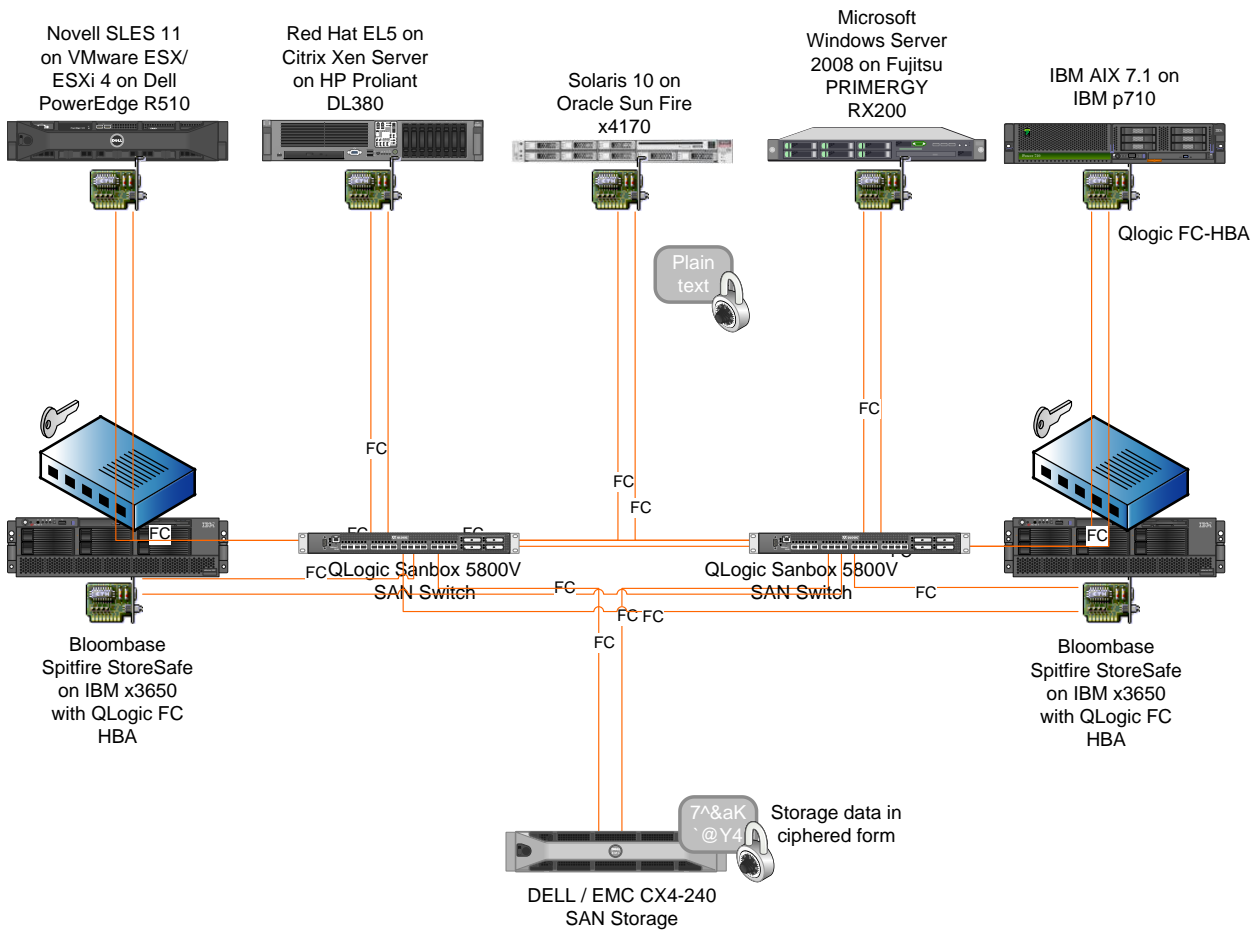
This document describes interoperability testing of QLogic powered Bloombase StoreSafe Security Server appliance on SAN storage sub-system. Therefore, it is assumed that you are familiar with operation of storage systems and major operating systems including Linux, Windows, AIX, HP-UX and Solaris. It is also assumed that you possess basic UNIX administration skills. The examples provided may require modifications before they are run under your version of UNIX.

As QLogic FC-HBA(s) and SAN switches are hardware option to Bloombase StoreSafe storage encryption system, you are recommended to refer to installation and configuration guides of specific model of QLogic FC-HBA 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 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



Bloombase StoreSafe Storage Encryption Server Appliance

Server	IBM eServer xSeries x3650 M3
Processors	2 x Intel Xeon 5600-series quad-core 3.6 GHz
Memory	8 GB
Operating System	Bloombase SpitfireOS 5.5 – Hardened and customized OS based on Linux kernel version 2.6.26 64-bit
Storage Encryption Software	Bloombase StoreSafe Security Server

Fiber Channel Host Bus Adapters

Model	QLogic QLE2672	QLogic QLE2562	QLogic QLE2462	QLogic QLA2342
Speed	16 Gbps	8 Gbps	4 Gbps	2 Gbps
Interface	PCI-E	PCI-E	PCI-E	PCI-X

SAN Switch

Model	2 x QLogic Sanbox 5800V Fabric SAN Switch
Link Speed	8/4/2 Gbps auto-sensing

Storage Area Network (SAN)

IP SAN Storage	Dell / EMC CX4-240 SAN Storage
Link Speed	8/4/2 Gbps auto-sensing

Storage Hosts

Model	Dell PowerEdge R510	HP Proliant DL380	Oracle Sun Fire x4170	Fujitsu PRIMERGY RX200	IBM p710
Operating System	Novell SLES 11 on VMware ESX/ESXi 4	Red Hat EL5 on Citrix XenServer	Solaris 10	Microsoft Windows Server 2008	IBM AIX 7.1
Host Bus Adapter	QLogic QLE2562	QLogic QLE2562	QLogic QLE2562	QLogic QLE2562	QLogic QLE2562

Optical Fiber Cables

Model	CommScope Systimax OM3 LC-LC patch cords	Corning OM3 LC-LC patch cords
--------------	--	-------------------------------

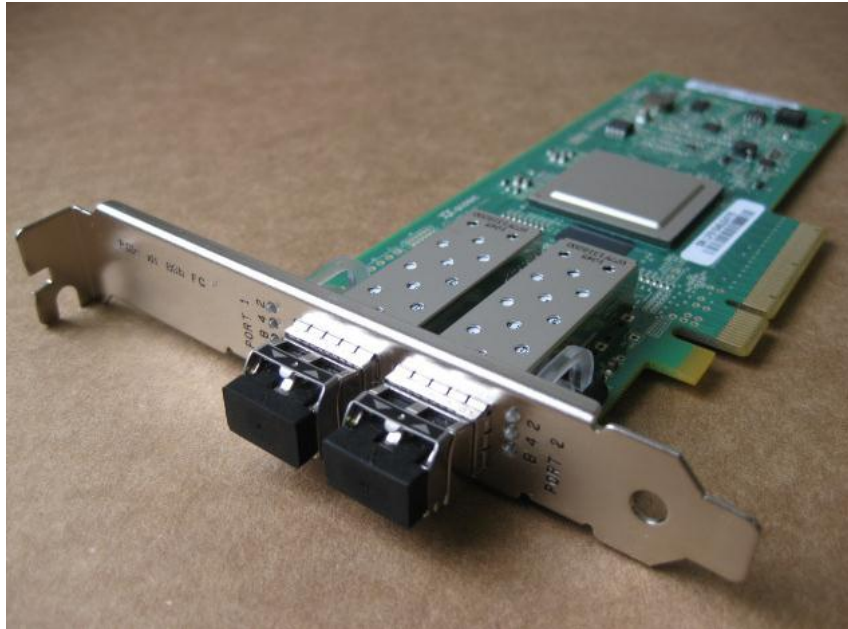
Configuration Overview

QLogic FC-HBA

QLogic FC-HBAs

- QLogic QLE2672
- QLogic QLE2562
- QLogic QLE2462
- QLogic QLA2362

are installed onto the x86-based appliance running Bloombase SpitfireOS 5.5.



SAN Fabric

The virtual disks on Dell / EMC SAN are exposed to Bloombase StoreSafe appliance for access via QLogic Sanbox 5800V Fabric SAN Switch.

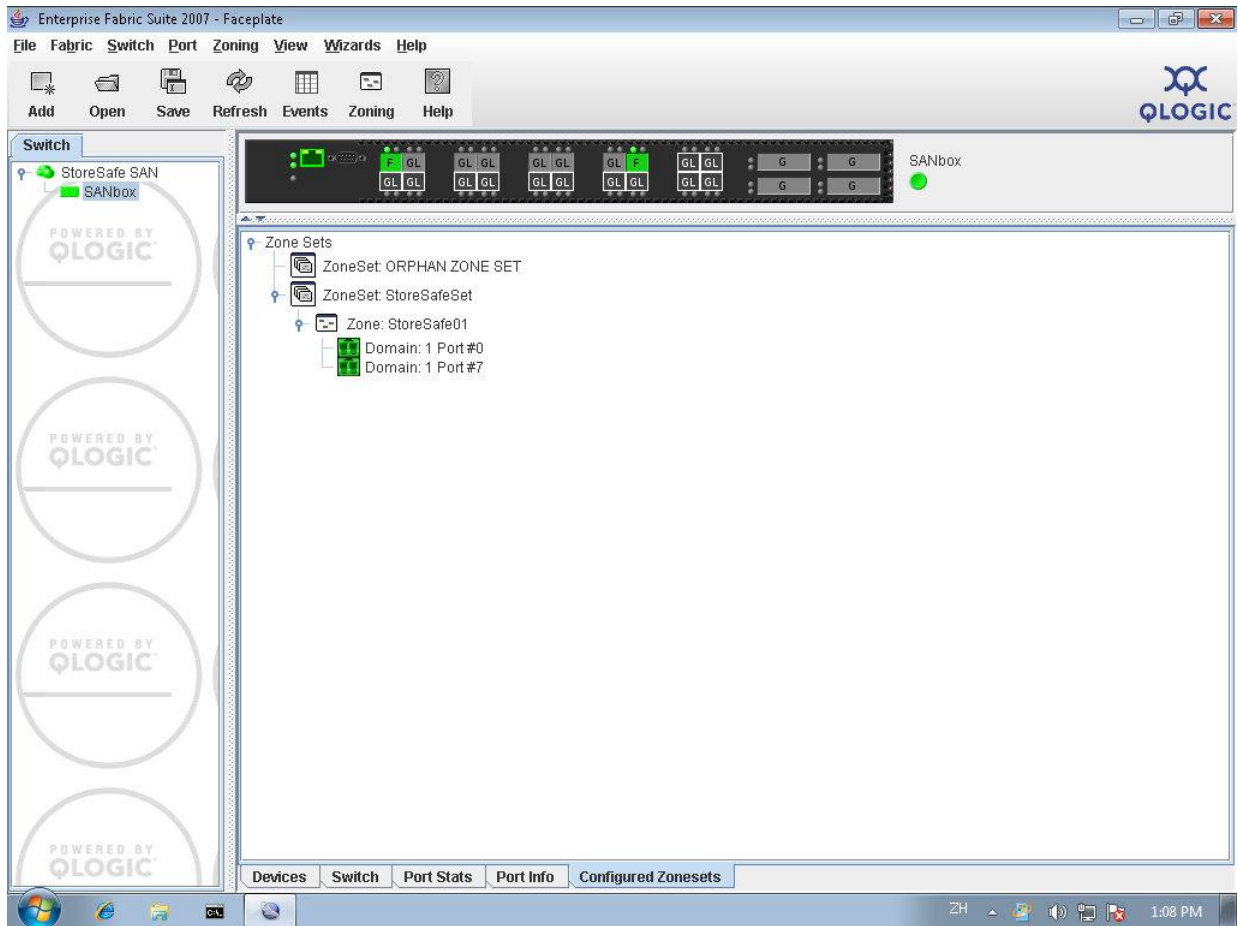
The screenshot displays the 'Enterprise Fabric Suite 2007 - Faceplate' application window. The interface includes a menu bar (File, Fabric, Switch, Port, Zoning, View, Wizards, Help) and a toolbar with icons for Add, Open, Save, Refresh, Events, Zoning, and Help. The QLOGIC logo is visible in the top right corner.

On the left side, there is a 'Switch' panel showing a tree view with 'StoreSafe SAN' and 'SANbox'. Below this are four circular logos with the text 'POWERED BY QLOGIC'.

The main area features a graphical representation of a SAN switch with various ports and connections. Below the switch diagram is a table with the following data:

Port WWN	Nickname	Details	FC Address	Switch	Port	Target/Initiator	Vendor	A
21:00:00:24:ff:17:cc			010000	SANbox	Port 0	Target	0x0024ff	Stor
10:00:00:00:c9:71:87:0c			010700	SANbox	Port 7	Initiator	EMULEX CORPORATION	Stor

At the bottom of the application window, there are tabs for 'Devices', 'Switch', 'Port Stats', 'Port Info', and 'Configured Zonesets'. The Windows taskbar at the very bottom shows the system tray with the time 1:07 PM.



SAN Storage

The screenshot shows a configuration window for SAN storage with the following sections:

- General** (selected tab):
 - Properties**: LUN Name: lun01, LUN ID: 01, Unique ID: 60:06:01:60:1E:80:29:00:E2:6C:53:C0:9B:8D:E0:11, Current State: Ready.
 - Operation In Progress**: Operation: (empty), Operation State: (empty), Refresh button.
 - Storage Pool Properties**: Storage Pool: Pool 0, RAID Type: RAID5, Drive Type: FC, Available Capacity: 3.000 GB.
 - LUN Capacity**: User Capacity: 3602.381 GB, Consumed Capacity: 3672.224 GB.
 - Advanced**: Alignment Offset: 0.
 - Ownership**: Auto Assignment Enabled, Current Owner: SP A, Allocation Owner: SP A, Default Owner: SP A, SP B.
- Buttons: OK, Apply, Cancel, Help.

A LUN is created at Dell / EMC CX4 SAN with below parameters

Name	lun01
Capacity	3 TB
Redundancy	RAID5

Optical Fiber Cables



Bloombase StoreSafe Security Server

Bloombase StoreSafe supports both file-based and block-based on-the-fly storage encryption. In this interoperability test exercise, fiber channel SAN block-based encryption is validated against QLogic FC-HBAs.

Bloombase Spitfire StoreSafe Security Server

Greeting
 Host Name: storesafe02
 User: admin
 Datetime: 2011-02-18 14:23:55 +0800

Menu Bar

- System
- Operation
- Network Security
- High Availability
- Administration
- Key Management
 - Spitfire KeyCastle
 - Hardware Security Module
 - Find Key Wrapper
 - Create Key Wrapper
- Storage

Language
 English

Find Key Wrapper

Name: Active:

CA:

Subject DN: Issuer DN:

Serial Number: Issuer Serial Number:

Effective Date From: Effective Date To:

Expiry Date From: Expiry Date To:

1-2 of 2

	Name	Key Source Type	Active	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1	kc-key01	Spitfire KeyCastle	<input checked="" type="checkbox"/>	<input type="checkbox"/>	CN=kc-key01	CN=kc-key01	2011-02-08 22:57:20 +0800	2021-02-05 22:57:20 +0800	2011-02-08 23:06:05 +0800
2	test	Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>	CN=test	CN=test	2011-02-08 22:40:51 +0800	2021-02-05 22:40:51 +0800	2011-02-08 22:40:54 +0800

1-2 of 2

Copyright © 2011 Bloombase Technologies


Encryption Key Configuration


Generate encryption key with name 'key' in bundled KeyCastle key life-cycle management tool

Modify Key Wrapper

Key Wrapper | Upload Key Contents | **Modify Key Source** | CRLDP | OCSP | Permissions

Modify Key Wrapper

Name	<input type="text" value="key"/>
Active	<input checked="" type="checkbox"/>
Exportable	<input type="checkbox"/>
CA	<input type="checkbox"/>
Subject DN	CN=key
Serial Number	695376542685815571917364
Issuer DN	CN=key
Certificate	<input checked="" type="checkbox"/> 
Public Key	<input checked="" type="checkbox"/>
Private Key	<input checked="" type="checkbox"/>
Key Bit Length	1024
Effective Datetime	2011-02-18 22:26:36 +0800
Expiry Datetime	2021-02-15 22:26:36 +0800
Revocation Check Method Type	<input type="text" value=""/> ▾
Revoked	<input type="checkbox"/>
Key Usage	-
Extended Key Usage	-
Owner	admin
Last Update Datetime	-



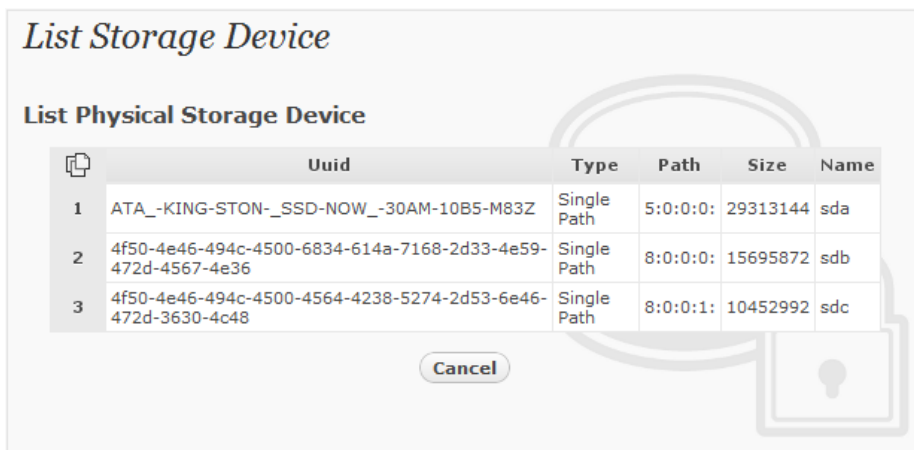
Virtual SAN Configuration

Bloombase StoreSafe block-based virtual storage and physical storage settings are configured as followings.



Physical Storage Target Configuration

After zoning and LUN mask are properly configured at SAN switches, StoreSafe should be able to mount to LUNs of SAN storages and shows on 'List Storage Device' tool



Physical storage namely 'luno1' is configured to map to the storage device to be encrypted by Bloombase StoreSafe

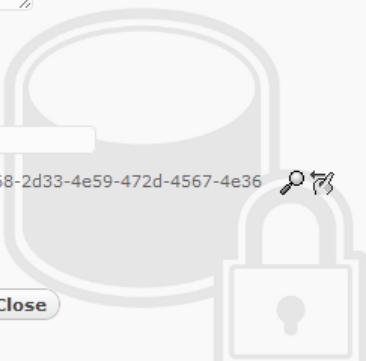
Bloombase StoreSafe secures SAN contents block by block. Volumes can be secured one by one by specific cryptographic cipher, bit length, encryption key, etc.

Modify Storage Configuration

Physical Storage | Permissions

Physical Storage Configuration

Name	<input type="text" value="lun01"/>
Description	<input type="text"/>
Physical Storage Type	Device <input type="button" value="v"/>
Type	<input type="text" value="FC"/>
Options	<input type="text"/>
Device	4f50-4e46-494c-4500-6834-614a-7168-2d33-4e59-472d-4567-4e36 <input type="button" value="m"/> <input type="button" value="l"/>
Owner	admin
Last Update Datetime	2011-02-18 18:06:54 +0800



Encrypted Virtual Storage Provisioning

Virtual storage namely 'san01' of type 'FC' is created to virtualize physical storage 'lun01' for transparent encryption protection over FCP

Modify Virtual Storage

Virtual Storage | **Protection** | Access Control | Permissions

Modify Virtual Storage

Name	<input type="text" value="san01"/>
Status	<input checked="" type="checkbox"/>
Description	<input type="text"/>
Active	<input checked="" type="checkbox"/>
Mode	FC <input type="button" value="v"/>
Owner	admin
Last Update Datetime	2011-02-19 02:46:25 +0800

Physical Storage

Storage	lun01 <input type="button" value="m"/> <input type="button" value="l"/>
Description	
Physical Storage Type	Device



Protection type is specified as 'Privacy' and secure the FC SAN LUN using AES-XTS 256-bit encryption with encryption key 'key'

Modify Virtual Storage Handler

Virtual Storage Protection Access Control Permissions

Virtual Storage Protection

Protection Type

Encryption Keys

	Key Name	Last Update Datetime
1	key	

Cryptographic Cipher

Cipher Algorithm

Bit Length

Fiber channel protocol access control relies mainly on LUN mask for host based access control, the WWN of host HBA on 'Host' of 'Host Access Control' section is configured as follows

Modify Virtual Storage Access Control

Virtual Storage Protection Access Control Permissions

Host Access Control

	Host	Last Update Datetime
1	10:00:00:00:c9:71:87:0c	2011-02-15 11:45:58 +0800

Validation Tests

Test Scenarios

Validation Matrix

Validation tests span across models of QLogic FC-HBAs and SAN switches, Bloombase StoreSafe Security Server, appliance hardware platform, and host platform.

Test Condition	Candidate
HBA	<ul style="list-style-type: none">• QLogic QLE2672• QLogic QLE2562• QLogic QLE2462• QLogic QLA2362
SAN Switch	<ul style="list-style-type: none">• QLogic Sanbox 5800V Fabric SAN Switch
Storage System	<ul style="list-style-type: none">• Dell / EMC CX4-240 SAN storage
Storage Encryption Appliance	<ul style="list-style-type: none">• Bloombase StoreSafe Security Server on x86-based IBM x3650

Host Server Hardware	<ul style="list-style-type: none"> • Dell PowerEdge R510 • HP Proliant DL-380 • Oracle Sun Fire x4170 • Fujitsu PRIMERGY RX200 • IBM p710
Host Operating Systems	<ul style="list-style-type: none"> • Microsoft Windows Server 2008 • Red Hat EL 5 • Novel SELS • Solaris 10 • IBM AIX • VMware ESX/ESXi (hypervisor) • Citrix XenServer (hypervisor)
Application Software	<ul style="list-style-type: none"> • Oracle Database 11g • Symantec Veritas Storage Foundation for Oracle RAC (SFRAC) 5.1

Raw Storage Device Tests

The following tests are carried out at storage host operating systems to access encrypted SAN storage via QLogic powered Bloombase StoreSafe appliances directly

Test	Description
Write disk with zeros	Write zeros into encrypted storage target via Bloombase StoreSafe, platform equivalence of UNIX's <code>dd if=/dev/zero of=/dev/sda</code>
Read disk to null device	Read from encrypted storage target via Bloombase StoreSafe, platform equivalence of UNIX's <code>dd if=/dev/sda of=/dev/null</code>
Wipe disk with random data	Write random zeros and ones into encrypted storage target, platform equivalence of UNIX's <code>dd if=/dev/urandom of=/dev/sda</code>

File System Tests

The following tests are carried out at storage hosts to access encrypted SAN storage via QLogic powered Bloombase StoreSafe appliances via operating system file-systems

- ext3 and Symantec Storage Foundation for Linux
- NTFS for Microsoft Windows
- JFS and Symantec Storage Foundation for IBM AIX
- UFS and Symantec Storage Foundation for Solaris

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
File permission configurations	<ul style="list-style-type: none"> • Platform equivalence of UNIX's chmod • Valid for UNIX-based storage host systems only (Linux, AIX, HPUX, Solaris)
Softlink/Symbolic link removal	<ul style="list-style-type: none"> • Platform equivalence of UNIX's rm • Valid for UNIX-based storage host systems only (Linux, AIX, HPUX, Solaris)
Softlink/Symbolic link move	<ul style="list-style-type: none"> • Platform equivalence of UNIX's mv

- Valid for UNIX-based storage host systems only (Linux, AIX, HPUX, Solaris)

Application Tests – Oracle Database Server on Symantec Veritas Storage Foundation for Oracle RAC

Test	Remarks
Database creation	Version equivalence of CREATE DATABASE
Schema 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

Result

Raw Storage Device Tests

Test	Validation Pass	Remarks
Write disk with zeros	✓	
Read disk to null device	✓	
Wipe disk with random data	✓	

File System Tests

Test	Validation Pass	Remarks
Directory creation	✓	
Directory rename	✓	
Directory removal	✓	
Directory move	✓	
File creation	✓	
File rename	✓	
File removal	✓	
File move	✓	
File append – by character	✓	
File append – by block	✓	
File parameters inquiry	✓	
File permission configurations	✓	
Softlink/Symbolic link removal	✓	
Softlink/Symbolic link move	✓	

Application Tests – Oracle Database Server on Symantec Veritas Storage Foundation for Oracle RAC

Test	Validation Pass	Remarks
Database creation	✓	
Schema creation	✓	
Database record insert	✓	
Database record query	✓	
Database record update	✓	
Database record delete	✓	

Index creation	✓
Tablespace alteration	✓
Redo log creation	✓
Redo log rotation	✓
Archive log creation	✓

Conclusion

QLogic FC-HBAs

- QLogic QLE2672
- QLogic QLE2562
- QLogic QLE2460
- QLogic QLA2362

and QLogic SAN switches

- QLogic Sanbox 5800V Fabric SAN switch

pass all Bloomberg InteropLab's interoperability tests with Bloomberg StoreSafe enterprise storage encryption server on file system access, Oracle Database applications and Symantec Storage Foundation for Oracle RAC (SFRAC).

Bloomberg Product	Operating System	QLogic FC-HBAs	QLogic SAN Switches
Bloomberg StoreSafe Security Server	Microsoft Windows Server 2008	QLE2672, QLE2562, QLE2460, QLE2362	QLogic Sanbox 5800V SAN Switch
	Red Hat Enterprise Linux 5	QLE2672, QLE2562,	QLogic Sanbox 5800V SAN

	QLE2460, QLE2362	Switch
Novel SELS 11	QLE2672, QLE2562, QLE2460, QLE2362	QLogic Sanbox 5800V SAN Switch
Solaris 10	QLE2672, QLE2562, QLE2460, QLE2362	QLogic Sanbox 5800V SAN Switch
IBM AIX 7	QLE2672, QLE2562, QLE2460, QLE2362	QLogic Sanbox 5800V SAN Switch
VMware ESX/ESXi 4 (hypervisor)	QLE2672, QLE2562, QLE2460, QLE2362	QLogic Sanbox 5800V SAN Switch
Citrix Xen Server (hypervisor)	QLE2672, QLE2562, QLE2460, QLE2362	QLogic Sanbox 5800V SAN Switch

Acknowledgement

We would like to thank QLogic Corporation for sponsoring and supporting the FC-HBAs and SAN switches used in tests of this technical report.

Disclaimer

The tests described in this paper were conducted in the Bloomberg InteropLab. Bloomberg 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 StoreSafe Security Server Technical Specifications, <http://www.bloombase.com/content/8936QA88>
2. Bloombase StoreSafe Security Server Compatibility Matrix, <http://www.bloombase.com/content/e8Gzz281>
3. dd for Microsoft Windows, <http://software.intel.com/en-us/articles/dd-for-windows/>
4. Oracle database server, www.oracle.com/us/products/database
5. Transaction Processing Performance Council, <http://www.tpc.org/tpcc/>
6. QLogic FC-HBAs, <http://www.qlogic.com/Products/adapters/Pages/FibreChannelAdapters.aspx>
7. QLogic Fiber Channel switches, <http://www.qlogic.com/Products/Switches/Pages/FibreChannelSwitches.aspx>
8. Symantec Veritas Storage Foundation for Oracle RAC, <http://www.symantec.com/storage-foundation-for-oracle-rac>