# **interop**Lab

# Encryption of Oracle Databases by Bloombase StoreSafe on NEC Express5800/ft Series Fault-Tolerant Server Application Notes

A Quick Guide to Deploy Bloombase StoreSafe on an NEC Express5800/ft Series Fault-Tolerant Server for encryption of Oracle Database

**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 NEC Express5800/ft series fault-tolerant server to achieve transparent Oracle encryption meeting various information security regulatory compliance standards without sacrificing performance.





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.

© 2008 Bloombase, Inc.

Bloombase, Spitfire, StoreSafe and Keyparc are either registered trademarks or trademarks of Bloombase in the United States, People's Republic of China, Hong Kong Special Administrative Region and/or other countries.

NEC is a registered trademark of NEC Corporation.

Oracle is a registered trademark of Oracle Corporation and / or its affiliates.

Microsoft and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and / or other countries.

Red Hat and Red Hat Enterprise Linux are registered trademarks of Red Hat Inc. in the United States and / or other countries

# **Table of Contents**

**Table of Contents** 

Introduction	5
Purpose and Scope	7
Infrastructure	8
Software	.8
Oracle Database Server	.8
Bloombase Spitfire StoreSafe Server	.9
Configuration Overview	10
Encryption of Oracle data files by Spitfire StoreSafe on Microsoft Windows 200	3, virtual storage connected by CIFS 12
Preparation for the Oracle server	12
Create Spitfire StoreSafe virtual storage for encryption	14
Migrate Oracle data files	19
Automatic failover testing	-
Encryption of Oracle data files by Spitfire StoreSafe on Microsoft Windows 200	3, virtual storage connected by NFS 20
Configuration of Microsoft Windows Services for UNIX	
Preparation for the Oracle server	
Create Spitfire StoreSafe virtual storage for encryption	
Migrate Oracle data files	
Automatic failover testing	28

3

Encryption of Oracle data files by Spitfire StoreSafe on Red Hat Enterprise Linux 4, virtual storage connected by CIFS

	-
Preparation for the Oracle server	29
Create Spitfire StoreSafe virtual storage for encryption	31
Migrate Oracle data files	
Automatic failover testing	37
Encryption of Oracle data files by Spitfire StoreSafe on Red Hat Enterprise	Linux 4, virtual storage connected by NFS
	38
Configuration of Microsoft Windows Services for UNIX	
Preparation for the Oracle server	-
Create Spitfire StoreSafe virtual storage for encryption	
Migrate Oracle data files	
Automatic failover testing	-
Automatic Failover of Oracle server	
Conclusion	49
Acknowledgement	50
Ackilowieugement	20
Disclaimer	51
	-
Technical Reference	52

# 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, hackerproof 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 Microsoft Windows and Red Hat Enterprise Linux platforms 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 Microsoft Windows and Red Hat Enterprise Linux operating system with the utilization of NEC Express5800/ft series fault-tolerant server.

# Infrastructure

### Software

Oracle Database

Bloombase Spitfire StoreSafe Server Bloombase StoreSafe storage security server 3.0

Oracle Databaser Server 8.1.7

### **Oracle Database Server**

Server

NEC Express5800/320Fd

Processors

Operating System

Quad-core 3.0GHz Microsoft Windows Server 2003 RC2 Enterprise Edition

## **Bloombase Spitfire StoreSafe Server**

Server

NEC Express5800/320Fc

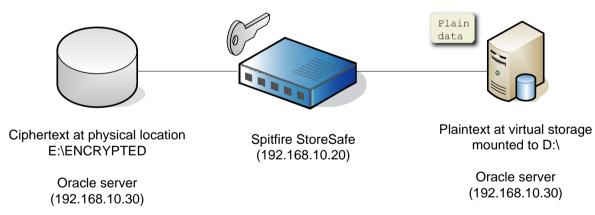
Processors

Quad-Core 2.66Hz

**Operating System** 

Microsoft Windows Server 2003 RC2 Enterprise Edition / Red Hat Enterprise Linux 4

# **Configuration Overview**



To demonstrate the full interoperability of Spitfire StoreSafe on NEC Express5800/ft series fault-tolerant server, we will perform the testing in 4 different scenario :

- 1. Encryption of Oracle data files on Microsoft Windows 2003 by Spitfire StoreSafe 3.0 on Microsoft Windows 2003, virtual storage connected by CIFS
- 2. Encryption of Oracle data files on Microsoft Windows 2003 by Spitfire StoreSafe 3.0 on Microsoft Windows 2003, virtual storage connected by NFS

- 3. Encryption of Oracle data files on Microsoft Windows 2003 by Spitfire StoreSafe 3.0 on Red Hat Enterprise Linux 4, virtual storage connected by CIFS
- 4. Encryption of Oracle data files on Microsoft Windows 2003 by Spitfire StoreSafe 3.0 on Red Hat Enterprise Linux 4, virtual storage connected by NFS

Before we start, assume the Oracle server is installed in the NEC Express5800/ft series fault-tolerant server with IP

and hostname

Spitfire StoreSafe is installed in another NEC Express5800/ft series server with IP

192.168.10.20

FC DEMO

and hostname

An Oracle instance is created and named

DB01

data files are stored at the local drive :

D:\ORACLE\ORADATA

What we aim to achieve is to have all the Oracle data files to get secured by Spitfire StoreSafe

In the testing regarding NFS connection, to connect Spitfire StoreSafe virtual storage by NFS in Microsoft Windows platform, Windows Services for UNIX needs to be installed. In this testing, we install Windows Services for UNIX 3.5

192.168.10.30

FTDEMO

### Encryption of Oracle data files by Spitfire StoreSafe on Microsoft Windows 2003, virtual storage connected by CIFS

### Preparation for the Oracle server

To start with, shutdown Oracle Instance first.

for user connection from Spitfire StoreSafe server.

To backup the original oracle data files, copy		
	D:\ORACLE	
to another drive eg		
	C:\TEMP	
To create a location for encrypted files eg		
	E:\ENCRYPTED	
, change the drive letter for the partition		
	D:	
to another drive		
	E:	
Create a windows user eg		
	ssuser	

😂 E:\encrypted		
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	<u>T</u> ools	Help
🔇 Back 🝷 🕤 👻 🏂 🔎 Se	earch 뗞	🏷 Folders 🛛 🕼 🌶 🗙 🏹 🔛 🕇
Address 🛅 E:\encrypted		
Folders	×	Name A
🞯 Desktop		
🗆 😑 My Documents		
🗉 🗄 🔂 SQL Server Managen	nent Stuc	
표 🚞 Visual Studio 2005		
🗉 😼 My Computer		
🕀 🥯 Local Disk (C:)		
🖃 🥯 Local Disk (E:)		
📄 💭 encrypted		

Share the encrypted file location to the windows user and grant with appropriate access permission.

encrypted Properties	? ×
	Permissions for encrypted ? X Share Permissions Group or user names: Susser (FTDEMO\ssuser)
User limit: <u>Maximum allowed</u> Allow this number of u To set permissions for users who access t folder over the network, click Permissions To configure settings for offline access, cl Caching.	Add     Bernove       Permissions for ssuser     Allow     Deny       Full Control     Image     Image       Change     Image     Image       Read     Image     Image
ОКС	OK Cancel Apply

ncrypted Properties		? ×
General Sharing Security C	ustomize	
Group or user names:		
Administrators (FTDEMOV	Administrators)	
CREATOR OWNER		
🕵 ssuser (FTDEMO\ssuser)		
🕵 SYSTEM		
🕵 Users (FTDEMO\Users)		
	A <u>d</u> d	<u>R</u> emove
Permissions for ssuser	Allow	Deny
Full Control		
Modify		
Read & Execute		
List Folder Contents		
Read	$\checkmark$	
Write		
Coopiel Permissions		
<ul> <li>For special permissions or for ac click Advanced.</li> </ul>	ivanceo settings,	Advanced
		1
OK	Cancel	Apply

### Create Spitfire StoreSafe virtual storage for encryption

#### Create an encryption key

Find Key Wra	pper					
Find Key W	rapper					
Name				Acti	ve	
CA		*				
Subject DN				Issu	er DN	
Serial Number				Issu	er Serial N	lu
Effective Date	From			Effe	ctive Date	Т
Expiry Date Fr	om			Exp	iry Date To	
			Fine	d Res	et Ad	đ
名 <sub>Name</sub>	Key Source Type	Active	CA	Subject DN	Issuer DN	1
1 key1	Local			CN=key1	CN=key1	

Create a storage configuration to the encrypted files physical location

Modify Storage Confi	guration
Storage Configura	tion
Modify Storage Co	nfiguration
Name	encryptedstorage
Description	
Physical Storage Type	Remote
Туре	CIFS 🗸
Options	user=ssuser,password=123456
Device	\\192.168.10.30\encrypted
Last Update Datetime	
	Submit Delete Close

#### Create a storage user

ssuser

who has the same name as the windows user

Modify Storage User	eSafe Security Server - Web A	^
Modify User		
User Id	ssuser	
Password	•••••	
Confirm Password	•••••	
Last Update Datetime		
Submit	Delete Close	

Create a virtual storage for the above storage configuration

Virtual Storage	Virtual Storage Handler Storage Access Control
Virtual Storage	Virtual Storage Halluler Storage Access Collition
Modify Virtual Sto	rage
Name	protected
Description	
Active	
Mode	File
Last Update Datetime	
Physical Storage	
	0.52
Storage	encryptedstorage 🔑 🕅
Description	
Physical Storage Type	Remote

Choose the defined encryption key and the appropriate cryptographic cipher

C Bloombase Spitfire	StoreSafe Security Server	- Web Man	agement Console	e - Windows I		×
Modify Virtual S	itorage Handler				^	Ĥ
Virtual Stora	ge Virtual Storage	Handler	Storage Acce	ss Control		
Virtual Storag	e Security Handling					
Security Scheme	Privacy 🗸					
Encryption Ke	eys					
2	Key Name	La	st Update Datet	ime		
1	key1					
	Add	Remove				
Cryptographi	c Cipher					
Cipher Algorithm	AES					
Bit Length	256 💙					
	Refresh	Close		T		◄

Grant the user access to the defined storage user so that Oracle instance can connect to the Spitfire StoreSafe virtual storage

C Bloombase Spitf	ire StoreSafe	Security Server - Web Manag	gement Console - Windows I	
Host Acces	ss Control			<b></b>
~	Host	Access Control List	Last Update Datetime	
		Add Remove		
Subnet Ac	cess Conti	rol		
2	Subnet	Access Control List	Last Update Datetime	
		Add Remove		
User Acces	ss Control			
Default	🗌 Rea	d 🗖 Write		
User Reposito	iry Local		~	L
2	User	Access Control List	Last Update Datetime	
1 🗖	ssuser 💙	🔽 Read 🔽 Write		
		Add Remove		▼

On the Spitfre StoreSafe server machine, change Bloombase Spitfire StoreSafe service to log on as the defined windows user

	Name (	Description	Chabur	Charles Trung	Line On An
Bloombase Spitfire StoreSafe	Name A	Description	Status	Startup Type	Log On As
Security Server	Alert Manager ALIVE(S) Service			Manual	Local System
	🎇 Alert Manager Main Service		Started	Automatic	Local System
<u>Start</u> the service	🍓 Alert Manager Socket(S) Service			Manual	Local System
	🎇 Alerter	Notifies sel		Disabled	Local Servio
Description:	🏶 Application Experience Lookup Service	Processes	Started	Automatic	Local System
Bloombase Spitfire StoreSafe Security Server	🆓 Application Layer Gateway Service	Provides s		Manual	Local Service
Server	🆓 Application Management	Processes i		Manual	Local System
	🏶 Automatic Updates	Enables th	Started	Automatic	Local System
	🍓 Background Intelligent Transfer Service	Transfers		Manual	Local System
	Bloombase Spitfire StoreSafe Security Server	Bloombase		Automatic	.\ssuser

Bloombase Spitfire Sto	reSafe Security Server Properties (Local <mark>?</mark> 🗙
General Log On Rec	overy Dependencies
Log on as:	
Local System according to Local System ac	unt interact with desktop
Ihis account	Assuser Browse
Password:	•••••
<u>C</u> onfirm password:	•••••
You can enable or disa	ble this service for the hardware profiles listed below:
Hardware Profile	Service
Profile 1	Enabled
	<u>Enable</u> <u>Disable</u>
	OK Cancel Apply

Back to the Oracle server machine, also change the Oracle instance service and Oracle TNS listener to log on as the windows user

<u>File Action View</u>	Help				
⇔ → 🛛 🖬 🖌	à 🗟 😫 🖬 🕨 🗉 🗉 🕬				
🎭 Services (Local)	Name 🛆	Description	Status	Startup Type	Log On As
	CracleOraHome81TNSListener			Automatic	.\ssuser
	OracleServiceDB01			Automatic	.\ssuser
	Reformance Logs and Alerts	Collects pe	Started	Automatic	Network S
	🆓 Plug and Play	Enables a c	Started	Automatic	Local System
	🐐 🙀 Portable Media Serial Number	Retrieves t		Manual	Local System
	Rrint Spooler	Manages al	Started	Automatic	Local System

After completed the virtual storage configuration and restarted Spitfire StoreSafe server, connect to the Spitfire StoreSafe virtual storage protected



#### Migrate Oracle data files

to

Encrypt the Oracle data files by copying the file from

Startup Oracle instance service and listener. With the Oracle data files location unchanged and connected as

D:\ORACLE

C:\TEMP

D:

, the Oracle instance can be started up successfully.

#### Automatic failover testing

To test the failover functionality of NEC Expess FT server, the power cable of the Spitfire StoreSafe server is unplugged to simulate a server down situation. While 10000 records are being encrypted by Spitfire StoreSafe server and inserted into the database, the server down and automatic failover provided by NEC Express5800/ft series fault-tolerant server has made the outage negligible throughout the data encryption process.



### Encryption of Oracle data files by Spitfire StoreSafe on Microsoft Windows 2003, virtual storage connected by NFS

#### **Configuration of Microsoft Windows Services for UNIX**

Create mapping between the users in Microsoft Windows platform and UNIX platform. Since Microsoft Windows does not use uid / gid like UNIX does, we will map the windows users to the immediate uid of -2 and gid of -2 which are the unmapped id in UNIX.

hicrosoft Windows Services for U	XIX		
🚡 Eile Action View Window He	þ		_ 5
← → 🗈 🖬 🔮 🖬			
Microsoft Windows Services for UNIX Server for NFS Client for NFS User Name Mapping	User Name Mapping on local computer Configuration Maps Map Maintenan Windows domain name: VFTDEMO List Windows Users Windows Users: Windows Users Windows Users Users SUPPORT_388545a0 Windows user name: Ssuser To create a map, enter user names you want to map, Advanced maps are listed below. To display simple below. If multiple Windows user names are mapped to the primary. To set a map to be the primary map, sete Mapped users: Windows User UNIX Doma in UNIX Use Windows User VYFTDEMOVESUSER VUNIX Doma in UNIX Use VYFTDEMOVESUSER	List UNIX users: UNIX users: UNIX users UNIX users UNIX users UNIX user ame UNIX user name: UNIX user name: Cummapped> and click Add. The Mapped users list, select to one UNIX user name, you must sele ect the map and click Set Primary.	

The Microsoft Windows Services for UN	IX	
🚡 Eile Action View Window Help		
		· · · · · · · · · · · · · · · · · · ·
		Eeload Apply ance List UNIX Groups UNIX groups: Unix Groups Gunmapped> -2 adm 48 bin 1 cunmapped> -2 daemon 2 dia UNIX group name: <unmapped> apply UNIX group name: <unmapped> apply Cunmapped&gt; -2 adm 48 bin 1 cunmapped&gt; -2 adm 48 bin 1 cunmapped&gt; -2 adm 48 bin 1 cunmapped&gt; -2 adm 48 bin 1 cunmapped&gt; -2 adm 48 bin 1 cunmapped&gt; -2 adm 48 bin 1 cunmapped&gt; -2 adm 48 bin 1 cunmapped&gt; -2 adm 48 bin 1 cunmapped&gt; -2 adm 48 bin 48 bin 48 bin 48 bin 48 bin 48 bin 48 bin 48 bin 48 bin 48 cunma 48 bin 48 cunma 48 bin 48 bin 48 bin 48 bin 48 cunma 48 bin 48 cunma 48 cunma 48 cunma 48 cunma 48 cunma 48 cunma 48 cunma 48 cunma 48 cunma 48 cunma 48 cunma 48 cunma 48 cunma 48 cunma 48 cunma 48 cunmapped&gt; adm 48 cunmapped&gt; adm 48 cunmapped&gt; adm 48 cunmapped&gt; adm 48 cunmapped&gt; adm 48 cunmapped&gt; adm 48 cunmapped&gt; adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm 48 cunmapped adm adm adm adm adm adm adm ad</unmapped></unmapped>
	below. If multiple Windows group names are mappe be the primary. To set a map to be the primary map, Mapped groups:	ed to one UNIX group name, you must select one map to , select the map and click Set Primary.
	Windows Group UNIX Domain UNIX Gr	roup Gid Prim
	¥¥FTDEMO¥ORA_DBA PCNFS (unmapp	ped> −2 * Set Primary Remov <u>e</u>

### Preparation for the Oracle server

To start with, shutdown Oracle Instance first.

To backup the original oracle data files, copy

to another drive eg

C:\TEMP

D:\ORACLE

To create a location for encrypted files eg

E:\ENCRYPTED

, change the drive letter for the partition

to another drive

Е:

Create a windows user eg

ssuser

for user connection from Spitfire StoreSafe server.



Share the encrypted file location to the windows user and grant with appropriate access permission

encrypted Properties	? ×		
General Sharing Security Customize You can share this folder with other network. To enable sharing for th folder. Do pot share this folder Share name: encrypted Comment:	Permissions for encrypted Share Permissions Group or user names: Susuer (FTDEMO\ssuser)		
User limit:	Permissions for ssuser Full Control Change Read	Add Allow V V	Bemove Deny
ОКС	ОК	Cancel	

crypted Properties		? >
General Sharing Security Cus	tomize	
Group or user names:		
Maninistrators (FTDEMO \Ac	ministrators)	
<b>11 CREATOR OWNER</b>		
🕵 ssuser (FTDEMO\ssuser)		
🕵 SYSTEM		
🕵 Users (FTDEMO\Users)		
	A <u>d</u> d	<u>R</u> emove
Permissions for ssuser	Allow	Deny
Full Control	V	
Modify	$\checkmark$	
Read & Execute	$\checkmark$	
List Folder Contents		
Read		ē
Write		
Consist Parmissions		
<ul> <li>For special permissions or for adva click Advanced.</li> </ul>	anced settings,	Advanced
olore randoa.	-	
	_	

### Create Spitfire StoreSafe virtual storage for encryption

Create an encryption key

Find Key Wrapp	er				
Find Key Wra	pper				
Name				Activ	ve
CA		*			
Subject DN				Issu	er DN
Serial Number				Issu	er Serial Nu
Effective Date Fro	m		_ 🔑	Effe	ctive Date T
Expiry Date From			_ <i>P</i>	Expi	iry Date To
			Find	d Res	et Add
A Name	Key Source Type	Active	CA	Subject DN	Issuer DN
1 key1	Local			CN=key1	CN=key1

Create a storage configuration to the encrypted files physical location

Storage Configura	tion	
Modify Storage Co	nfiguration	
Name	encryptedstorage	
Description		
Physical Storage Type	Remote	
Туре	CIFS 💌	
Options	user=ssuser,password=1234	56
Device	\\192.168.10.30\encrypted	
Last Update Datetime		

Create a virtual	storage for	r the above	storage	configuration

oombase Spitfire Stores	Safe Security Server - Web Management Console - Windows I 🔳 🗖
Modify Virtual Storag	je ^
Virtual Storage	Virtual Storage Handler Storage Access Control
Modify Virtual Stor	rage
Name	protected
Description	
Active	
Mode	File
Last Update Datetime	
Physical Storage	
Storage	encryptedstorage 🔑 🕅
Description	
Physical Storage Type	Remote
	Submit Delete Close

Choose the defined encryption key and the appropriate cryptographic cipher

lloombase Spitfire	StoreSafe Security Server	- Web Management	Console - Windows I	. 📃	
Modify Virtual S	torage Handler				
Virtual Stora	ge Virtual Storage I	tandler Storag	ge Access Control		
Virtual Storag	e Security Handling				
Security Scheme	Privacy 💙				
Encryption K	eys				
2	Key Name	Last Updat	te Datetime		
1	key1				
Cryptographi	Add Cipher	Remove			
Cipher Algorithm	AES 💌				
Bit Length	256 💙				
	Refresh	Close			

For the storage access control, specify the default user identifier and group identifier to the unmapped id -2 which is used for the mapping between the windows users identifier and the unix user identifiers.

Grant the host access to the Oracle server so that Oracle instance can connect to the Spitfire StoreSafe virtual storage

Virtual St	orage Vii	rtual Storage Handler	Storage Access Control
File Systen	n Object Attı	ributes	
Default User I	(dentifier -2		
Default Group			
Default Mode	73	77	
Host Acces	ss Control		
2	Host	Access Control List	Last Update Datetime
1	192.168.10.30	Read 🔽 Write	
Subnet Ac	cess Contro	Add Remove	
2	Subnet	Access Control List	Last Update Datetime
			1
		Add Remove	
User Acces	ss Control	Add Remove	
User Acces	ss Control ☑ <sub>Read</sub>	Add Remove	

On the Spitfre StoreSafe server machine, change Bloombase Spitfire StoreSafe service to log on as the defined windows user

🍇 Services (Local)	,				
Bloombase Spitfire StoreSafe	Name A	Description	Status	Startup Type	Log On As
Security Server	🏶 Alert Manager ALIVE(S) Service			Manual	Local System
	🆓 Alert Manager Main Service		Started	Automatic	Local System
<u>Start</u> the service	🆓 Alert Manager Socket(S) Service			Manual	Local System
	🖓 Alerter	Notifies sel		Disabled	Local Service
Description:	🍓 Application Experience Lookup Service	Processes	Started	Automatic	Local System
Bloombase Spitfire StoreSafe Security	🆓 Application Layer Gateway Service	Provides s		Manual	Local Service
Server	Application Management	Processes i		Manual	Local System
	n Automatic Updates	Enables th	Started	Automatic	Local System
	Background Intelligent Transfer Service	Transfers		Manual	Local System
	Bloombase Spitfire StoreSafe Security Server	Bloombase		Automatic	.\ssuser

Bloombase Spithre Sto	reSafe Security Server Properties (Local <mark>?</mark> 🗙
General Log On Rec	overy Dependencies
Log on as:	
C Local System acco	
Allo <u>w</u> service to	interact with desktop
• This account	.\ssuser Browse
Password:	•••••
<u>C</u> onfirm password:	••••••
	able this service for the hardware profiles listed below:
Hardware Profile	Service
Hardware Profile	Service
Hardware Profile	Service Enabled
Hardware Profile	Service
Hardware Profile	Service Enabled
Hardware Profile	Service Enabled

Back to the Oracle server machine, also change the Oracle instance service and Oracle TNS listener to log on as the windows user

🍇 Services					
<u>File Action View</u>	Help				
← → 💽 🗗 🗟	) 🗟 😫 🖬 🕨 🗉 🗉 🕬				
🍇 Services (Local)	Name 🛆	Description	Status	Startup Type	Log On As
	🍓 OracleOraHome81TNSListener			Automatic	.\ssuser
	CracleServiceDB01			Automatic	.\ssuser
	🎇 Performance Logs and Alerts	Collects pe	Started	Automatic	Network S
	🆏 Plug and Play	Enables a c	Started	Automatic	Local System
	🍓 Portable Media Serial Number	Retrieves t		Manual	Local System
	Print Spooler	Manages al	Started	Automatic	Local System

After completed the virtual storage configuration and restarted Spitfire StoreSafe server, connect to the Spitfire StoreSafe virtual storage protected

\$ mount 192.168.10.20:/protected D:

One of the benefits of NFS connection is the hard mount options, which will keep the re-establishing the lost connection infinitely.

\$ mount		
Local	Remote	Properties
D:	\192.168.10.20\protected	UID=-2, GID=-2 rsize=32768, wsize=32768 mount=hard, timeout=0.8 retry=1, locking=no fileaccess=777, lang=ANSI casesensitive=no

### Migrate Oracle data files

Encrypt the Oracle data files by copying the file from

to

C:\TEMP

D:

Startup Oracle instance service and listener. With the Oracle data files location unchanged and connected as

D:\ORACLE

, the Oracle instance can be started up successfully.

#### Automatic failover testing

To test the failover functionality of NEC Expess FT server, the power cable of the Spitfire StoreSafe server is unplugged to simulate a server down situation. While 10000 records are being encrypted by Spitfire StoreSafe server and inserted into the database, the server down and automatic failover provided by NEC Express5800/ft series server has made the outage negligible throughout the data encryption process.

C:\Documents and Settings\Walter\My Documents\projects\demo-storesafe-db\classes>java -cp .:/lib/mysql-connector-java-3.0.10-stable-bin.jar:/lib/hsqldb.
/lib/ifxjdbcx.jar PopulateData oracle.jdbc.driver.OracleDriver "jdbc:oracle:thin:@192.168.10.30:1521:db01" orabm 10000 false
Done with 0 card records Done with 1000 card records
Jone with 1000 card records
Done with 3000 card records
Done with 4000 card records
Done with 5000 card records Done with 8000 card records
Jone with SUDU card records
Done with 8000 card records
Done with 9000 card records
All done with 10000 card records

## Encryption of Oracle data files by Spitfire StoreSafe on Red Hat Enterprise Linux 4, virtual storage connected by CIFS

Preparation for the Oracle server		
To start with, shutdown Oracle Instance first.		
To backup the original oracle data files, copy		
	D:\ORACLE	
to another drive eg		
	C:\TEMP	
To create a location for encrypted files eg		
	E:\ENCRYPTED	
, change the drive letter for the partition		
	D:	
to another drive		
	E:	
Create a windows user eg		
create a windows user eg		
	ssuser	
for user connection from Spitfire StoreSafe server.		

E:\encrypted					
<u>File E</u> dit <u>V</u> iew F <u>a</u> vor	ites <u>T</u> ools	<u>H</u> elp			
😋 Back 🝷 🕤 👻 🥬	🗅 Search  🦻	> Folders	B (	¥ 🗶	₽
Address 🛅 E:\encrypted					
Folders	×	Name 4			
🞯 Desktop					
🗉 🚞 My Documents					
🗄 🗄 🔂 SQL Server Man	🗉 🛅 SQL Server Management Stud				
🗉 🗄 🔁 Visual Studio 200	🗄 🧰 Visual Studio 2005				
🗉 😼 My Computer					
🗄 🥯 Local Disk (C:)					
🖃 🥯 Local Disk (E:)					
📄 💭 📄 📄					

Share the encrypted file location to the windows user and grant with appropriate access permission

encrypted Properties	? ×	
General Sharing Security Customize	Permissions for encrypted	? ×
You can share this folder with othe network. To enable sharing for th folder.  Do not share this folder  Share this folder  Share name: encrypted Comment: User limit:  Maximum allowed C Allow this number of u	Group or user names:	e
To set permissions for users who access t folder over the network, click Permissions To configure settings for offline access, cl Caching.	Permissions for ssuser Allow Deny Full Control Change	
ОК С	OK Cancel Ar	ply

Administrators (FTDEM	1\Administrators)	
CREATOR OWNER		
😨 ssuser (FTDEMO\ssuse	er)	
🕵 SYSTEM		
🕵 Users (FTDEMO\Users	)	
1	A <u>d</u> d	<u>R</u> emove
Permissions for ssuser	Allow	Deny
Full Control		
Modify	$\checkmark$	
Read & Execute		
List Folder Contents		
Read	$\checkmark$	
Write		

### Create Spitfire StoreSafe virtual storage for encryption

Create an encryption key

Find Key Wrapper						
Find Key Wra	pper					
Name				Acti	ve	
CA		*				1
Subject DN	Subject DN					
Serial Number				Issu	er Serial N	iu
Effective Date Fro	m		_ <i>/</i> 2	Effe	ctive Date	Т
Expiry Date From			<i>~</i>	Exp	ry Date To	
Find Reset Add						
A Name	Key Source Type	Active	CA	Subject DN	Issuer DN	1
1 key1	Local			CN=key1	CN=key1	

Create a storage configuration to the encrypted files physical location

Modify Storage Configuration				
Storage Configura	tion			
Modify Storage Co	nfiguration			
Name	encryptedstorage			
Description				
Physical Storage Type	Remote			
Туре	CIFS 💌			
Options	user=ssuser,password=123456			
Device	\\192.168.10.30\encrypted			
Last Update Datetime				
	Submit Delete Close			

Create a storage user

ssuser

who has the same name as the windows user

🖉 Bloombase Spitfire Sto	reSafe Security Server - V	Veb Ma 🔳 🗖 🔀
Modify Storage Use	er	^ <b>^</b>
Modify User		
User Id	ssuser	
Password	•••••	
Confirm Password	•••••	
Last Update Datetime		
Submit	t Delete Close	

Create a virtual storage for the above storage configuration

Modify Virtual Stora	Je ^
Virtual Storage	Virtual Storage Handler Storage Access Control
Modify Virtual Sto	rage
Name	protected
Description	
Active	<b>v</b>
Mode	File
Last Update Datetime	
Physical Storage	
Storage	encryptedstorage 🔑 😿
Description	
Physical Storage Type	Remote
	Submit Delete Close

Choose the defined encryption key and the appropriate cryptographic cipher

<i>(</i> B	loombase Spitfire	StoreSafe Security Server	- Web Management Console	- Windows I		k
	Modify Virtual S	itorage Handler				-
	Virtual Stora	ge Virtual Storage	Handler Storage Access	s Control	_	
	Virtual Storag	e Security Handling				
	Security Scheme	Privacy 🗸				
	Encryption Ke	eys				
	2	Key Name	Last Update Dateti	me		
	1	key1				
	<b>Cryptographi</b> Cipher Algorithm Bit Length	Add AES 256 V Refrest	Remove			

Grant the user access to the defined storage user so that Oracle instance can connect to the Spitfire StoreSafe virtual storage

🌈 Bloombase Spitf	ire StoreSafe	Security Server - Web Manag	gement Console - Windows I		
Host Acces	ss Control			<b></b>	
2	Host	Access Control List	Last Update Datetime	]	
	Add Remove				
Subnet Ac	cess Conti	rol			
2	Subnet	Access Control List	Last Update Datetime		
Add Remove					
User Acces	ss Control				
Default	🗌 Rea	d 🗖 Write			
User Reposito	ry Local		~		
2	User	Access Control List	Last Update Datetime	]	
1	ssuser 💌	🗹 Read 🔽 Write			
		Add Remove		•	

On the Spitfre StoreSafe server machine, change Bloombase Spitfire StoreSafe service to log on as the defined windows user

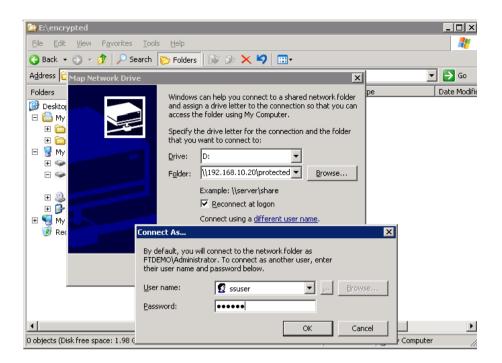
🍇 Services (Local)					
Bloombase Spitfire StoreSafe	Name A	Description	Status	Startup Type	Log On As
Security Server	🆓 Alert Manager ALIVE(S) Service			Manual	Local System
	🆓 Alert Manager Main Service		Started	Automatic	Local System
Start the service	🆓 Alert Manager Socket(S) Service			Manual	Local System
	🎇 Alerter	Notifies sel		Disabled	Local Service
Description:	🍓 Application Experience Lookup Service	Processes	Started	Automatic	Local System
Bloombase Spitfire StoreSafe Security Server	🎇 Application Layer Gateway Service	Provides s		Manual	Local Service
Derver	🎇 Application Management	Processes i		Manual	Local System
	🎇 Automatic Updates	Enables th	Started	Automatic	Local System
	🍓 Background Intelligent Transfer Service	Transfers		Manual	Local System
	Bloombase Spitfire StoreSafe Security Server	Bloombase		Automatic	.∖ssuser

Bloombase Spitfire StoreSafe Security	/ Server Properties (Local <mark>?</mark> 🗙
General Log On Recovery Depende	ncies
Log on as:	
Local System account     Allow service to interact with desk	top
• This account .\ssuser	Browse
Password:	•••••
Confirm password:	•••••
You can enable or disable this service fo	r the hardware profiles listed below:
Hardware Profile	Service
Profile 1	Enabled
	Enable Disable
OK	Cancel Apply

Back to the Oracle server machine, also change the Oracle instance service and Oracle TNS listener to log on as the windows user



After completed the virtual storage configuration and restarted Spitfire StoreSafe server and the Oracle instance, connect to the Spitfire StoreSafe virtual storage protected



### Migrate Oracle data files

Encrypt the Oracle data files by copying the file from

C:\TEMP

D:

to

Startup Oracle instance service and listener. With the Oracle data files location unchanged and connected as

D:\ORACLE

, the Oracle instance can be started up successfully.

#### Automatic failover testing

To test the failover functionality of NEC Expess FT server, the power cable of the Spitfire StoreSafe server is unplugged to simulate a server down situation. While 10000 records are being encrypted by Spitfire StoreSafe server and inserted into the database, the server down and automatic failover provided by NEC Express5800/ft series fault-tolerant server has made the outage negligible throughout the data encryption process.



### Encryption of Oracle data files by Spitfire StoreSafe on Red Hat Enterprise Linux 4, virtual storage connected by NFS

### **Configuration of Microsoft Windows Services for UNIX**

Create mapping between the users in Microsoft Windows platform and UNIX platform. Since Microsoft Windows does not use uid / gid like UNIX does, we will map the windows users to the root uid of o and gid of o in UNIX.

hicrosoft Windows Services for UNIX		
🚡 Eile Action View Window Help		
← → 🗈 🖬 😤 🖬		
Microsoft Windows Services for UNIX     Server for NFS     Client for NFS     Client for NFS     User Ners     User Name Mapping	User Name Mapping on local computer Configuration Maps Map Maintenan	
	To create maps, click Apply. User Name Mapping creat	_
	Advanced maps	
	To map user names, click Show User Maps. To map gr <u>Hide User Maps</u> <u>Show Group Maps</u> <u>W</u> indows domain name: \\FTDEMO <u>List \Windows Users</u>	bup names, click Show Group Maps. List UNIX Users
	Windows users: Vindows Users Cummapped> Administrator ASPNET Guest USR_320-FB IWAM_320-FB IWAM_320-FB SSUSER Windows user name: SSUSER	UNIX users: Unix Users: Unix Users Ntp 38 Operator 11 oracle 501 pcape 77 pegasus 66 peter 503 root 0 UNIX user name: root
User Name Mapping	ssuser To create a map, enter user names you want to map, a	·

hicrosoft Windows Services for UNIX			_ 🗆
🚡 Eile Action Yiew Window Help			_ 18
			· · · · · · · · · · · · · · · · · · ·
Microsoft Windows Services for UNIX     Server for NFS     Clent for NFS     User Name Mapping	User Name Mapping on local computer           Configuration         Maps         Map Maintenar           To map user names, click Show User Maps         Hide Group Maps         To map gr           Show User Maps         Hide Group Maps         Windows on map gr           Windows domain name:         Itel Group Maps         Itel Group Maps           Windows domain name:         Itel Group Maps         Itel Group Maps           Windows groups:         Itel Group Maps         Itel Group Maps           Windows groups:         Itel Group Maps         Itel Group Maps           Windows groups:         Itel Group Maps         Itel Group Maps           Windows group         Itel Group Maps         Itel Group Maps           Windows group for the set of the		Beload         Apply           up Maps.           List UNDX Groups           610           502           505           504           77           65           503           0
	To create a map, enter group names you want to map	, and click Add.	Add

#### Preparation for the Oracle server

To start with, shutdown Oracle Instance first.

To backup the original oracle data files, copy

D:\ORACLE

to another drive eg

C:\TEMP

To create a location for encrypted files eg

E:\ENCRYPTED

, change the drive letter for the partition

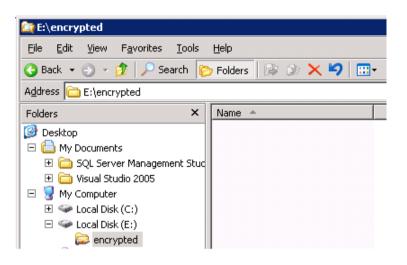
to another drive

D:

Create a windows user eg

ssuser

for user connection from Spitfire StoreSafe server.



Share the encrypted file location to the windows user and grant with appropriate access permission

encrypted Properties	? ×		
General       Sharing       Security       Customize         You can share this folder with othe network. To enable sharing for th folder.         Do not share this folder         Share this folder         Share name:       encrypted         Comment:       inclusion	Permissions for encrypted Share Permissions Group or user names: Susser (FTDEMO\ssuser)		? ×
User limit: <u>Maximum allowed</u> <u>Allow</u> this number of u To set permissions for users who access t folder over the network, click Permissions To configure settings for offline access, cl Caching.	Permissions for ssuser Full Control Change Read	Add Allow V V	Remove
ОКС	OK	Cancel	Apply

encrypted Properties		?	×
General Sharing Security Cust	omize		
<u>G</u> roup or user names:			
🙍 Administrators (FTDEMO \Adi	ministrators)		
CREATOR OWNER			
ssuser (FTDEMO\ssuser)			
SYSTEM			
🕵 Users (FTDEMO\Users)			
	1		
	A <u>d</u> d	<u>R</u> emove	
Permissions for ssuser	Allow	Deny	
Full Control			
Modify			
Read & Execute	$\checkmark$		
List Folder Contents			
Read			
Write			
Coocial Parmissions			
For special permissions or for adva click Advanced.	nced settings, _	Ad <u>v</u> anced	
OK	Cancel	Apply	

### Create Spitfire StoreSafe virtual storage for encryption

Create an encryption key

Find Key Wrapp	er					
Find Key Wra	pper					
Name				Acti	ve	
CA		*				
Subject DN				Issu	ier DN	
Serial Number				Issu	ier Serial N	lu
Effective Date Fro	m 🗌		<i>~</i>	Effe	ctive Date	Т
Expiry Date From			<i>,</i>	Exp	iry Date To	5
			Fin	d Res	et Ad	d
A Name	Key Source Type	Active	CA	Subject DN	Issuer DN	1
1 key1	Local			CN=key1	CN=key1	

Create a storage configuration to the encrypted files physical location

Modify Storage Confi	guration
Storage Configura	tion
Modify Storage Co	onfiguration
Name	encryptedstorage
Description	
Physical Storage Type	Remote
Туре	CIFS 💌
Options	user=ssuser,password=123456
Device	\\192.168.10.30\encrypted
Last Update Datetime	
	Submit Delete Close

Create a virtual	storage	for the	above	storage	configu	ıration
				000.030	· · · · · · · · · · · · · · · · · · ·	

Modify Virtual Stora	ge ^
Virtual Storage	Virtual Storage Handler Storage Access Control
Modify Virtual Sto	rage
Name	protected
Description	
Active	
Mode	File
Last Update Datetime	
Physical Storage	
Storage	encryptedstorage 🔑 📆
Description	
Physical Storage Type	Remote
	Submit Delete Close

Choose the defined encryption key and the appropriate cryptographic cipher

Modify Virtual	Storage Handler		
Virtual Stor	age Virtual Storag	ge Handler Storage Access Control	
Virtual Stora	ge Security Handlin	ıg	
Security Scheme	Privacy	×	
Encryption K	Keys		
2	Key Name	Last Update Datetime	
1	key1		
Cryptograph	Add	Remove	
Cipher Algorithm			
Bit Length	256 💙		

#### Grant the host access to the Oracle server so that Oracle instance can connect to the Spitfire StoreSafe virtual storage



On the Spitfre StoreSafe server machine, change Bloombase Spitfire StoreSafe service to log on as the defined windows user

Bloombase Spitfire StoreSafe	Name 🛆	Description	Status	Startup Type	Log On As
Security Server	Alert Manager ALIVE(S) Service			Manual	Local System
<u>Start</u> the service	🍓 Alert Manager Main Service		Started	Automatic	Local System
	🆓 Alert Manager Socket(S) Service			Manual	Local System
	🍓 Alerter	Notifies sel		Disabled	Local Servic
Description:	🍓 Application Experience Lookup Service	Processes	Started	Automatic	Local System
Bloombase Spitfire StoreSafe Security Server	🍓 Application Layer Gateway Service	Provides s		Manual	Local Service
berver	🆓 Application Management	Processes i		Manual	Local System
	🍓 Automatic Updates	Enables th	Started	Automatic	Local System
	🏶 Background Intelligent Transfer Service	Transfers		Manual	Local Syster
	Bloombase Spitfire StoreSafe Security Server	Bloombase		Automatic	.\ssuser

	,
Bloombase Spitfire StoreSa	fe Security Server Properties (Local <mark>?</mark> 🗙
General Log On Recover,	Dependencies
Log on per	
Log on as:	
C Local System account	
Allo <u>w</u> service to inter	act with desktop
• This account:	ssuser <u>B</u> rowse
Password:	
Confirm password:	•••••
You can enable or disable t	is service for the hardware profiles listed below:
Hardware Profile	Service
Profile 1	Enabled
,	
	<u>Enable</u>
	OK Cancel Apply

Back to the Oracle server machine, also change the Oracle instance service and Oracle TNS listener to log on as the windows user

🍇 Services						
<u>File Action View</u>	Help					
	à 🗟 😫 🖬 🕨 🗉 🗉 🕬					
🍇 Services (Local)	Name 🛆	Description	Status	Startup Type	Log On As	
	🖓 OracleOraHome81TNSListener			Automatic	.\ssuser	
	🐝 OracleServiceDB01			Automatic	.\ssuser	
	Reformance Logs and Alerts	Collects pe	Started	Automatic	Network S	
	🍓 Plug and Play	Enables a c	Started	Automatic	Local System	
	🖓 Portable Media Serial Number	Retrieves t		Manual	Local System	
	🆓 Print Spooler	Manages al	Started	Automatic	Local System	

After completed the virtual storage configuration and restarted Spitfire StoreSafe server, connect to the Spitfire StoreSafe virtual storage protected

```
$ mount 192.168.10.20:/protected D:
```

One of the benefits of NFS connection is the hard mount options, which will keep the re-establishing the lost connection infinitely.

\$ mount		
Local	Remote	Properties
D:	\192.168.10.20\protected	UID=-2, GID=-2 rsize=32768, wsize=32768 mount=hard, timeout=0.8 retry=1, locking=no fileaccess=777, lang=ANSI casesensitive=no

#### Migrate Oracle data files

to

Encrypt the Oracle data files by copying the file from

C:\TEMP D:

Startup Oracle instance service and listener. With the Oracle data files location unchanged and connected as

, the Oracle instance can be started up successfully.

### Automatic failover testing

To test the failover functionality of NEC Expess FT server, the power cable of the Spitfire StoreSafe server is unplugged to simulate a server down situation. While 10000 records are being encrypted by Spitfire StoreSafe server and inserted into the database, the server down and automatic failover provided by NEC Express5800/ft series fault-tolerant server has made the outage negligible throughout the data encryption process.



### **Automatic Failover of Oracle server**

Apart from the automatic failover of Spitfire StoreSafe server with the help of NEC Express5800/ft series fault-tolerant server, automatic failover of Oracle server on the powerful HA-enabled machine is also performed. To test the failover functionality of NEC Express FT server, the hardware module is unplugged to simulate a server down situation. At the same time, 10000 records are encrypted by Spitfire StoreSafe server and inserted into the database, the automatic failover provided by NEC Express5800/ft series fault-tolerant server has made the data encryption process continuous without a single moment of downtime, data loss and interruption to Spitfire StoreSafe security server. The user-transparent fault-tolerance of NEC's FT server has significantly improved the system availability.

Before the server outage, both the HA modules are in "System Duplexing" mode.

🖥 Server maintenance utility - System Information				
<u>File Yiew Settings Tool Help</u>				
№? 🛍				
■     FTDEMO       ■     System Configuration       ■     State Configuration	Chassis Information         Type :       Rack Mount Chassis         Part Number :       243413716         Serial Number :       01         System Information       05         DS :       Microsoft Windows Server 2003 Enterprise Edition         DS Version :       5.2.3790         Name :       FTDEMO         Product Information       Marufacturer :         Manufacturer :       NEC         Product :       NEC         Post Number :       ZAPUS5800/320Fb-LR [N8800-111F]         Serial Number :       ZAPUS130         Version :       FR1.5         LCD       Module #0         Module #0       Module #1         System Ready       System Ready			

After unplugged the server module to simulate a server down disaster, the running module will take over to be the active node and running in "Simplex" mode.

	Chassis Information Type : Rack Mount Chassis Part Number : 243-413716 Serial Number : 01
Generation (D11/1) Generation (D11/1) Generation (D11/1) Generation (D11/1) Generation (D11/1) Generation (D11/1)	System Information OS : Microsoft Windows Server 2003 Enterprise Edition OS Version : 5.2.3790 Name : FTDEMO
	Product Information           Manufacturer : NEC           Product : NEC           Part Number : Express5800/320Fb-LR [N8800-111F]           Serial Number : 7X00130           Version : FR1.5
	LCD Module #0 Module #1 System Simplex System Ready

## 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 NEC Express5800/ft Series Fault-Tolerant Server to achieve transparent Oracle encryption meeting high availability requirement and various information security regulatory compliance standards without sacrificing performance.

# 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 :

Lamson Chan, NEC IT Platform Infrastructure

Kevin Cheung, NEC IT Platform Infrastructure

# 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. NEC Express5800/ft Fault-Tolerant, http://www.nec.com/global/prod/express/library/brochure/ft\_Eo8FT2.pdf
- 2. Oracle Storage Program Change Notice, <u>http://www.oracle.com/technology/deploy/availability/htdocs/oscp.html</u>
- 3. Oracle Database Protection by Spitfire StoreSafe, <u>http://www.bloombase.com/download/index.jsp?Url=/products/spitfire/storeSafe/OracleDatabaseProtectionBy</u> <u>SpitfireStoreSafe.pdf</u>
- 4. Bloombase Spitfire StoreSafe Compatibility Matrix for NAS, http://www.bloombase.com/content/8396639C9Q8dkeo46yZ3i7Yvfa6iaCNvwpZ81x