 © 2008 Bloombase, Inc.

interopLab

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.

BLOOMBASE® NEC

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

 © 2008 Bloombase, Inc.

Table of Contents

Table of Contents 3

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 2003, 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 19
Encryption of Oracle data files by Spitfire StoreSafe on Microsoft Windows 2003, virtual storage connected by NFS 20
Configuration of Microsoft Windows Services for UNIX 20
Preparation for the Oracle server 21
Create Spitfire StoreSafe virtual storage for encryption 24
Migrate Oracle data files 28
Automatic failover testing 28

Encryption of Oracle data files by Spitfire StoreSafe on Red Hat Enterprise Linux 4, virtual storage connected by CIFS 29
Preparation for the Oracle server 29
Create Spitfire StoreSafe virtual storage for encryption 31
Migrate Oracle data files 36
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 38
Preparation for the Oracle server 39
Create Spitfire StoreSafe virtual storage for encryption 42
Migrate Oracle data files 46
Automatic failover testing 47
Automatic Failover of Oracle server 48

Conclusion 49

Acknowledgement 50

Disclaimer 51

Technical Reference 52

 © 2008 Bloombase, Inc.

Introduction

Digital assets including financial reports, legal documents, private human resources information, confidential contracts and sensitive user data are invaluable properties of a corporation. A business cannot risk losing these information, both confidentiality and non-repudiation. Nevertheless, the Internet has becoming more pervasive, security attacks have grown. News and reports have revealed millions of dollars of loss in various enterprises and organizations due to security breaches.

Data protection at the persistence layer used to be an uncommon subject in information technology industry. Persistence data, in the old days, are assumed safely kept and stored in highly secure data centers with effective physical access control and close surveillance. However, trends in the industry in backup, archive and high availability with an aim to safeguard data from the worst attack and be responsive to rescues, keeping the enterprise core system running non-stop, have opened up chances confidential data get disclosed and tampered by unauthorized parties.

Numerous security compliance and standards including Sarbanes Oxley, Gramm-Leach-Bliley Act and Personal Data Privacy Ordinance have raised enterprises' awareness of securing their core business and customer data. However, persistence data protection is technically a difficult subject. One has to prepare for additional system complexity, loss of performance, at the same time, maintaining the same level of stability and scalability, and most important of all, be highly secure, hacker-proof rather than exposing more security loopholes.

Core business data of an enterprise constitutes a major segment of assets that a corporation possesses. Customer data, marketing strategies, intellectual properties in form of source codes and business logic, sales history and prediction figures, and other decision support numerical analysis as result of data-mining may often bury forward looking intelligence that in some sense have very high future value when put into good use.

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

 © 2008 Bloombase, Inc.

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

 © 2008 Bloombase, Inc.

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.

 © 2008 Bloombase, Inc.

Infrastructure

Software

Oracle Database	Oracle Databaser Server 8.1.7
Bloombase Spitfire StoreSafe Server	Bloombase StoreSafe storage security server 3.0

Oracle Database Server

Server	NEC Express5800/320Fd
Processors	Quad-core 3.0GHz
Operating System	Microsoft Windows Server 2003 RC2 Enterprise Edition

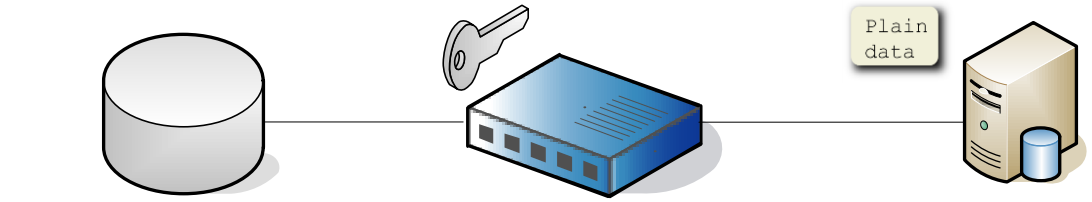
 © 2008 Bloombase, Inc.

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

 © 2008 Bloombase, Inc.

Configuration Overview



Ciphertext at physical location
E:\ENCRYPTED

Oracle server
(192.168.10.30)

Spitfire StoreSafe
(192.168.10.20)

Plaintext at virtual storage
mounted to D:\

Oracle server
(192.168.10.30)

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

 © 2008 Bloombase, Inc.

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

```
192.168.10.30
```

and hostname

```
FTDEMO
```

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

```
192.168.10.20
```

and hostname

```
FC_DEMO
```

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

 © 2008 Bloombase, Inc.

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.

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

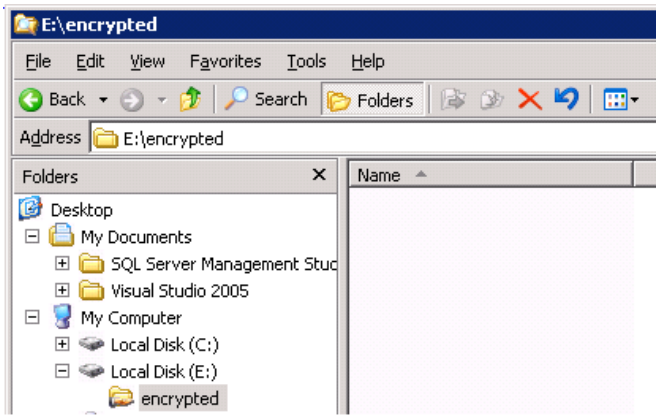
```
E:
```

Create a windows user eg

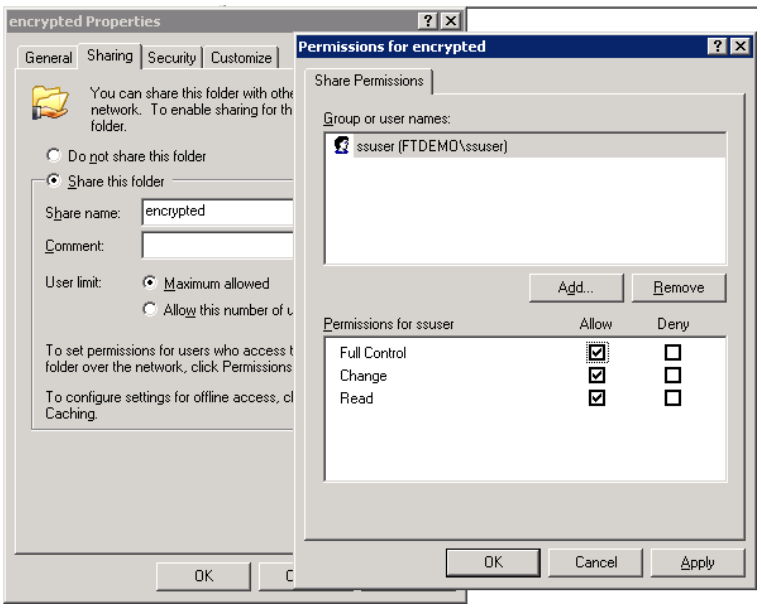
```
ssuser
```

for user connection from Spitfire StoreSafe server.

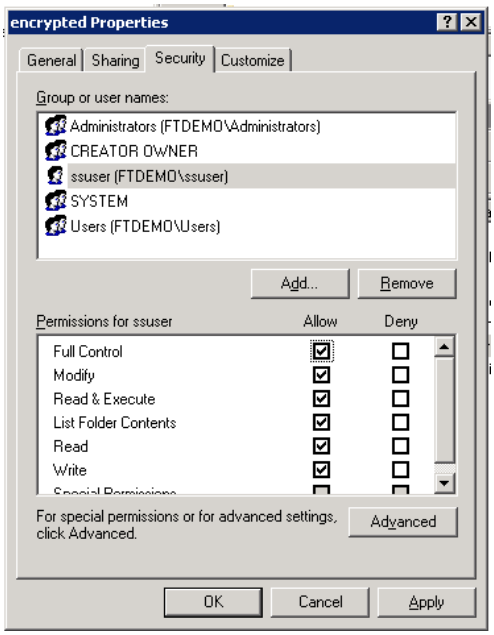
 © 2008 Bloombase, Inc.



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

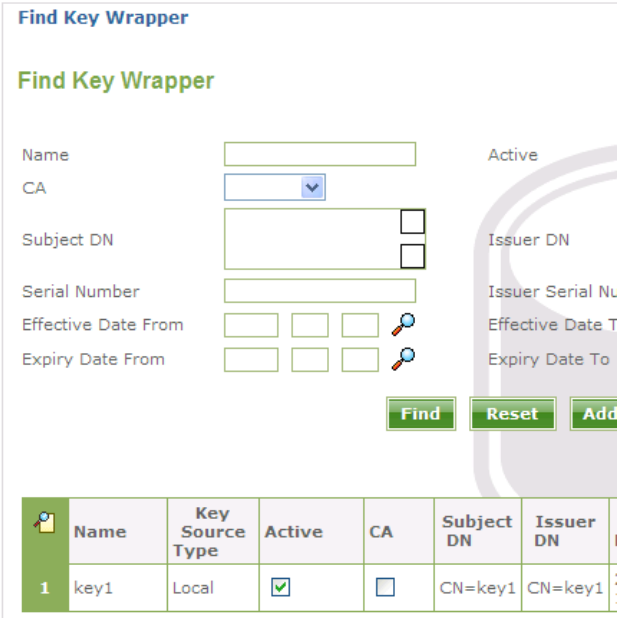


 © 2008 Bloombase, Inc.



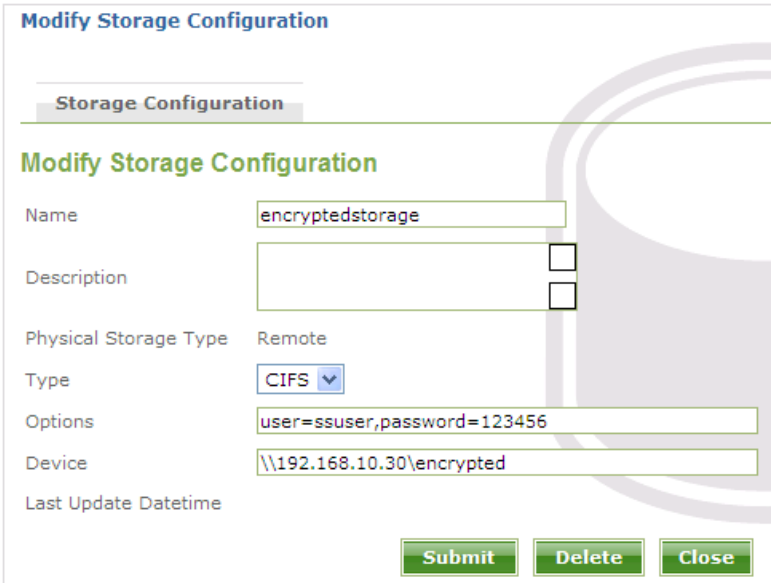
Create Spitfire StoreSafe virtual storage for encryption

Create an encryption key



Create a storage configuration to the encrypted files physical location

 © 2008 Bloombase, Inc.



 © 2008 Bloombase, Inc.

Create a storage user

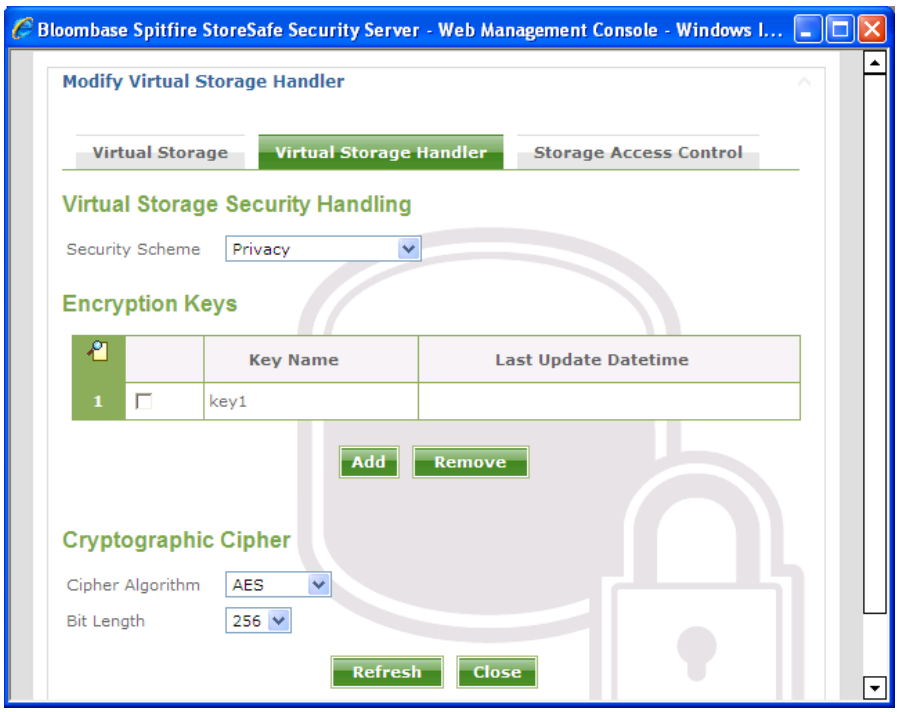
```
ssuser
```

who has the same name as the windows user

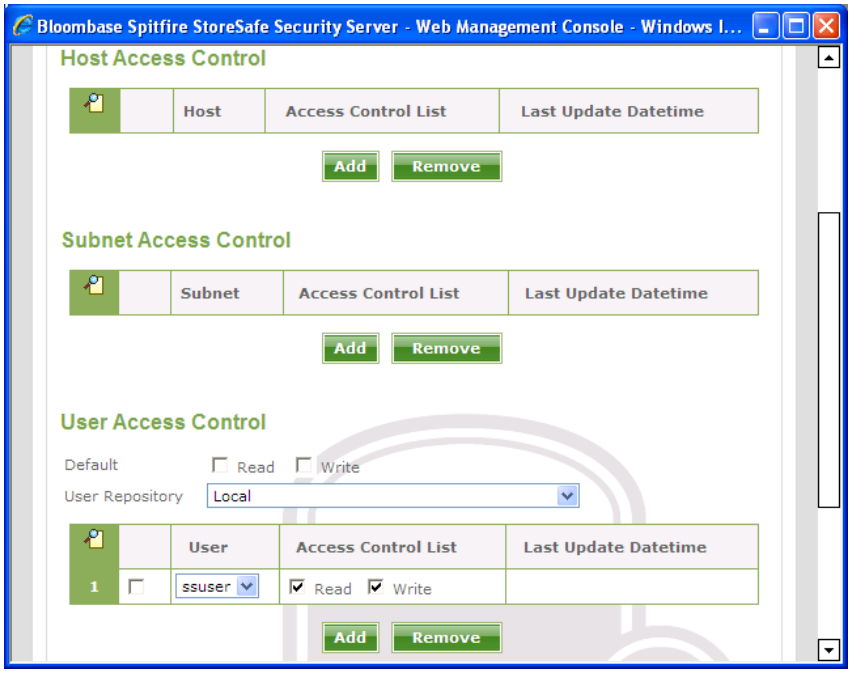
Create a virtual storage for the above storage configuration

 © 2008 Bloombase, Inc.

Choose the defined encryption key and the appropriate cryptographic cipher

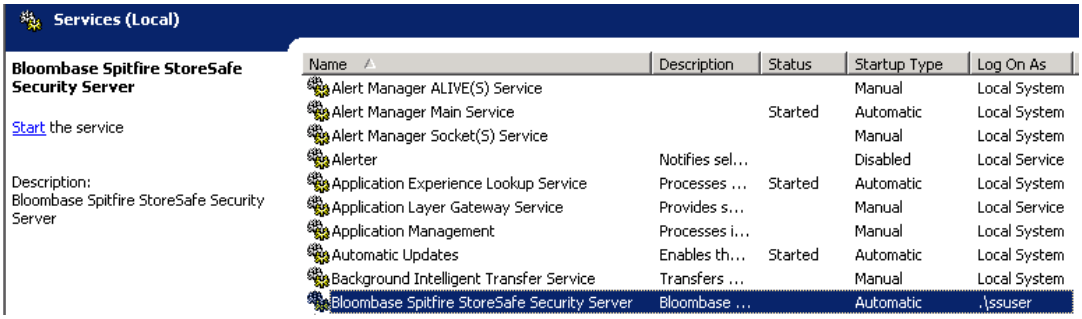


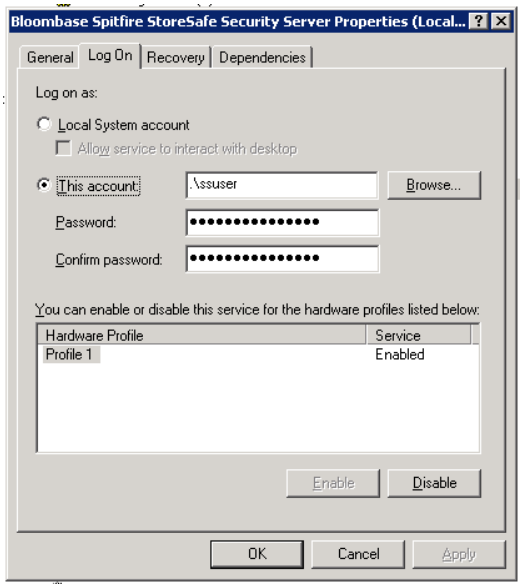
Grant the user access to the defined storage user so that Oracle instance can connect to the Spitfire StoreSafe virtual storage



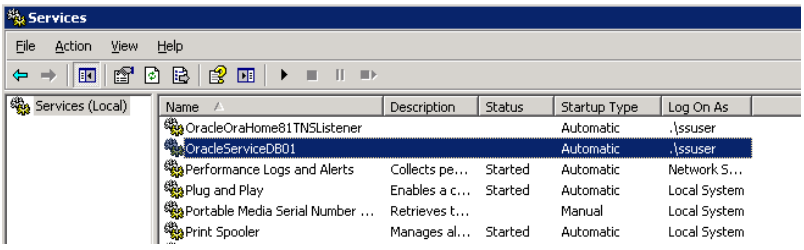
 © 2008 Bloombase, Inc.

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

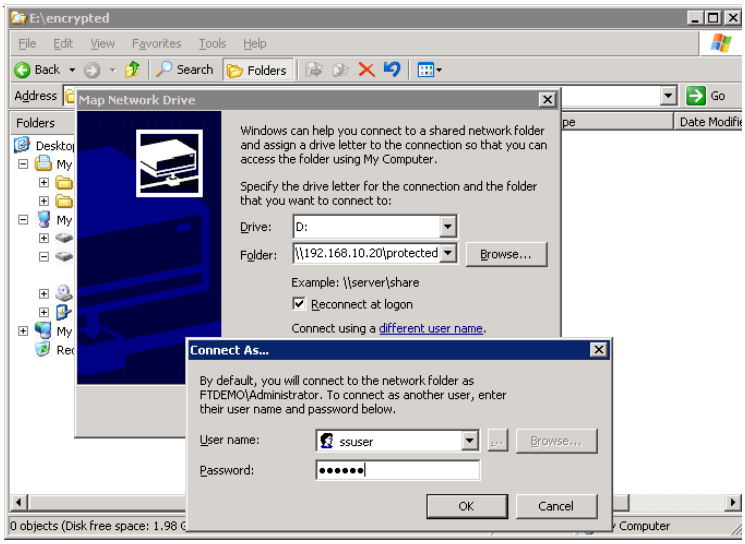




Back to the Oracle server machine, also change the Oracle instance service and Oracle TNS listener to log on as the windows user



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



Migrate Oracle data files

Encrypt the Oracle data files by copying the file from

```
C:\TEMP
```

to

```
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 fault-tolerant server has made the outage negligible throughout the data encryption process.

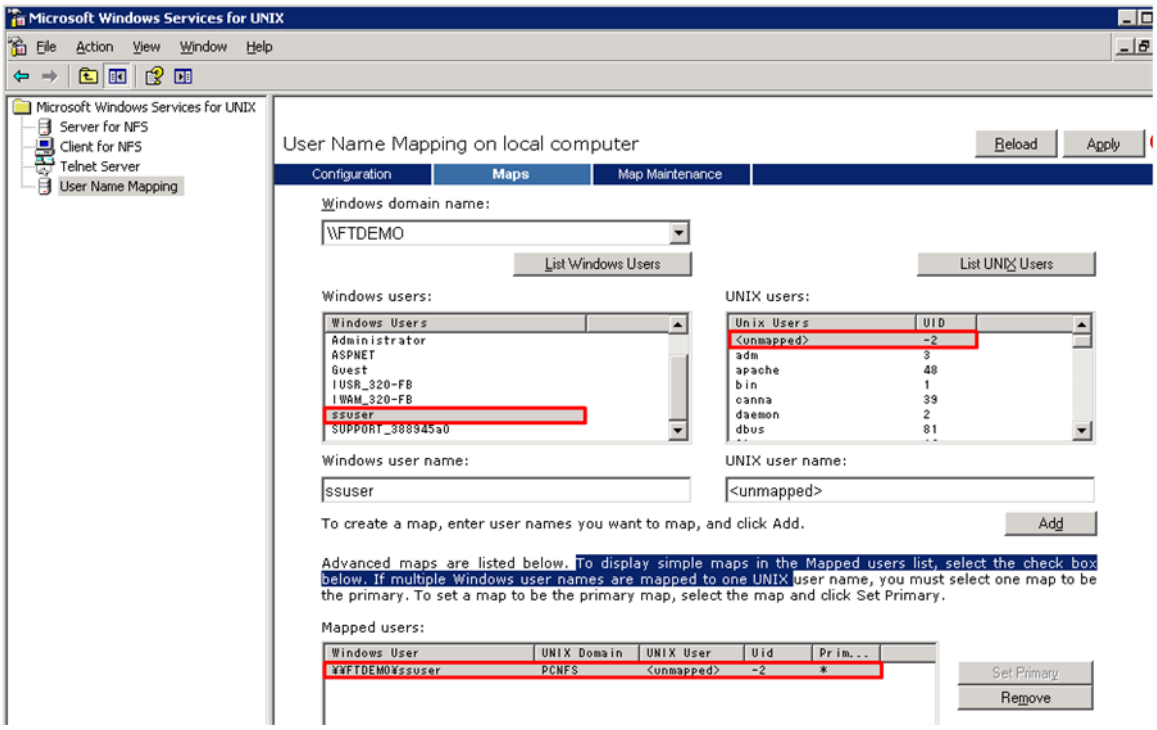
 © 2008 Bloombase, Inc.

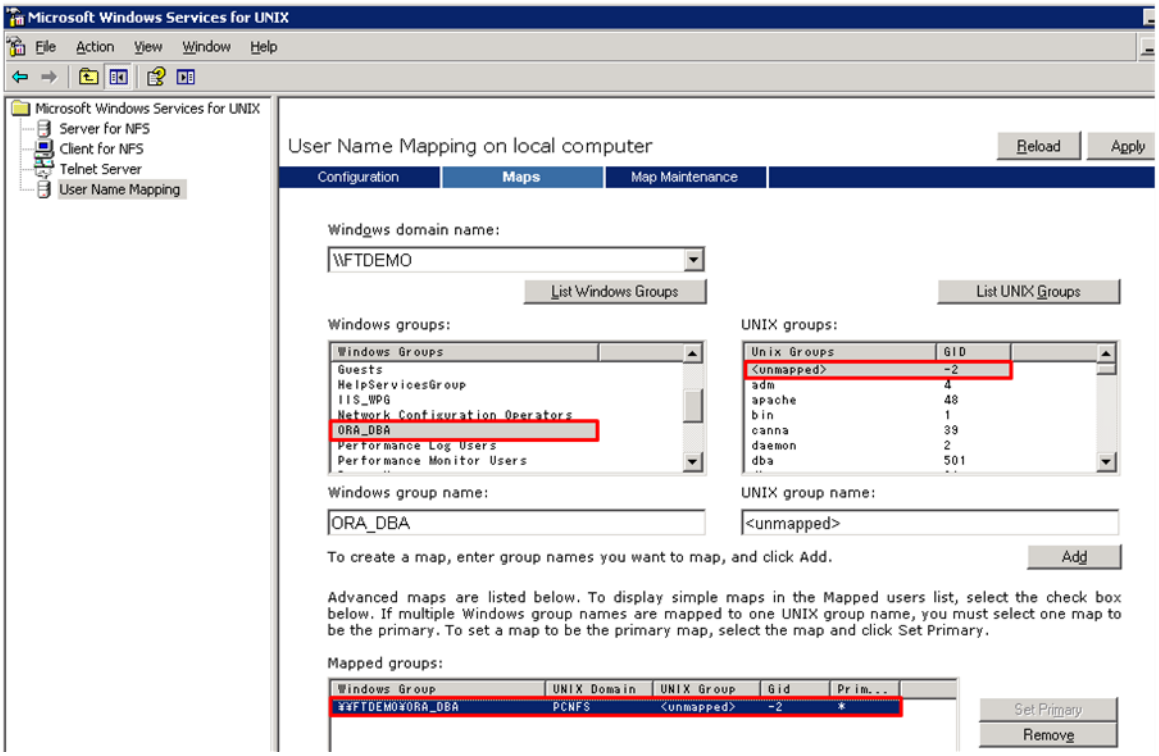
```
C:\Documents and Settings\Walter\My Documents\projects\demo-storesafe-db\classes>java -cp .;../lib/mysql-connector-java-3.0.10-stable-bin.jar;../lib/hsqldb.
/lib/ifxjdbcx.jar PopulateData oracle.jdbc.driver.OracleDriver "jdbc:oracle:thin:@192.168.10.30:1521:db01" orabm orabm 10000 false
Done with 0 card records
Done with 1000 card records
Done with 2000 card records
Done with 3000 card records
Done with 4000 card records
Done with 5000 card records
Done with 6000 card records
Done with 7000 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 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.





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:
```

 © 2008 Bloombase, Inc.

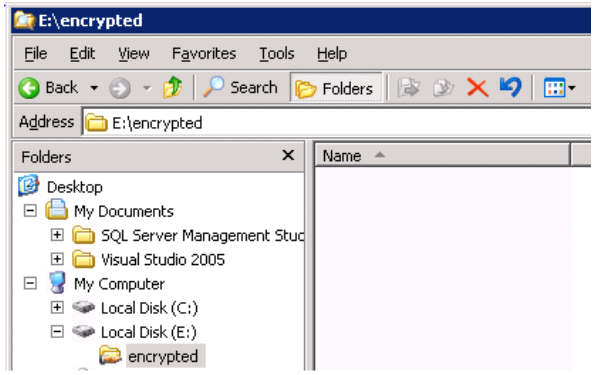
to another drive

```
E:
```

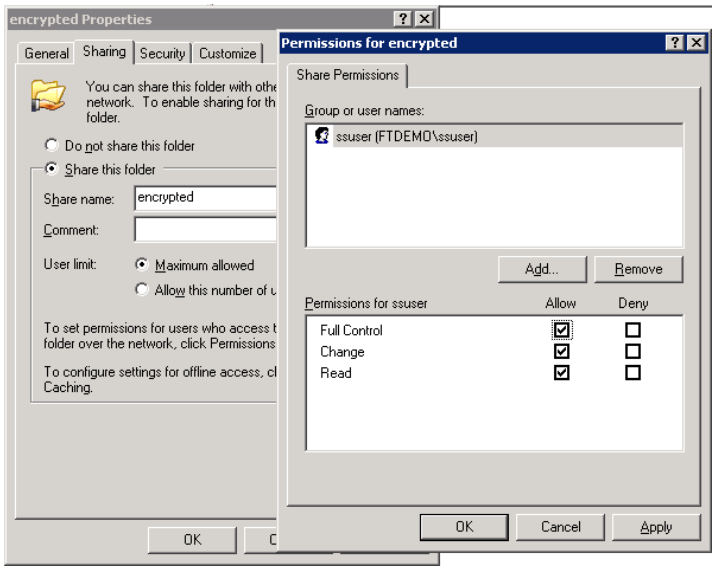
Create a windows user eg

```
ssuser
```

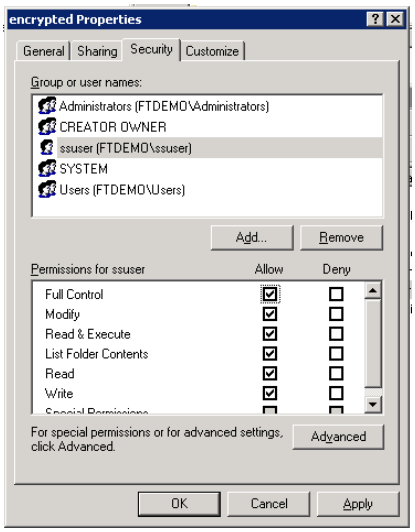
for user connection from Spitfire StoreSafe server.



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



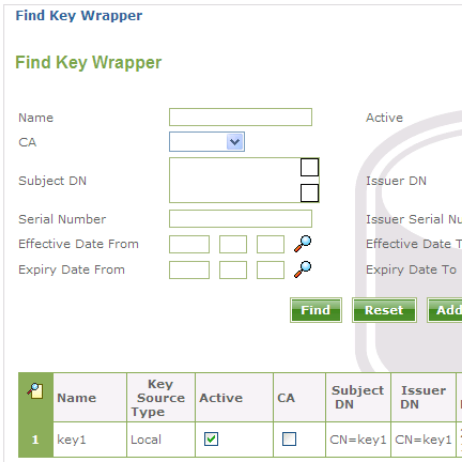
 © 2008 Bloombase, Inc.



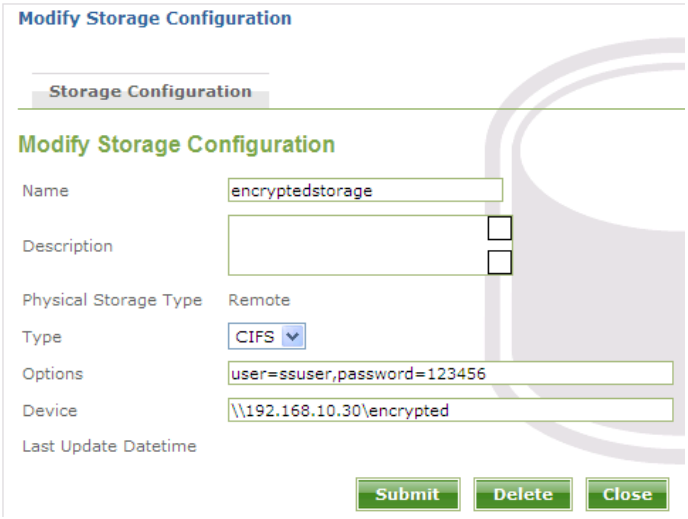
 © 2008 Bloombase, Inc.

Create Spitfire StoreSafe virtual storage for encryption

Create an encryption key



Create a storage configuration to the encrypted files physical location



 © 2008 Bloombase, Inc.

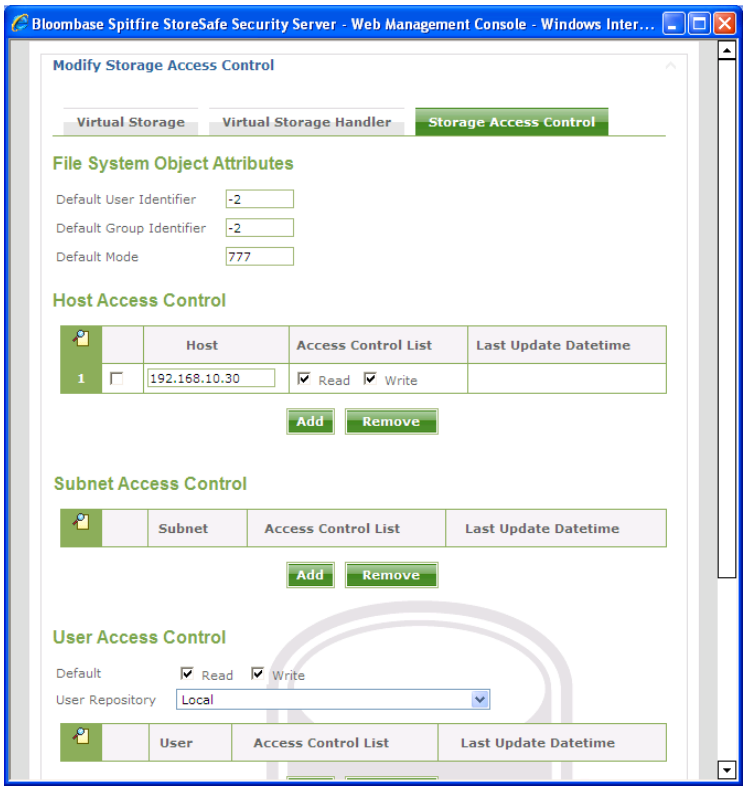
Create a virtual storage for the above storage configuration

Choose the defined encryption key and the appropriate cryptographic cipher

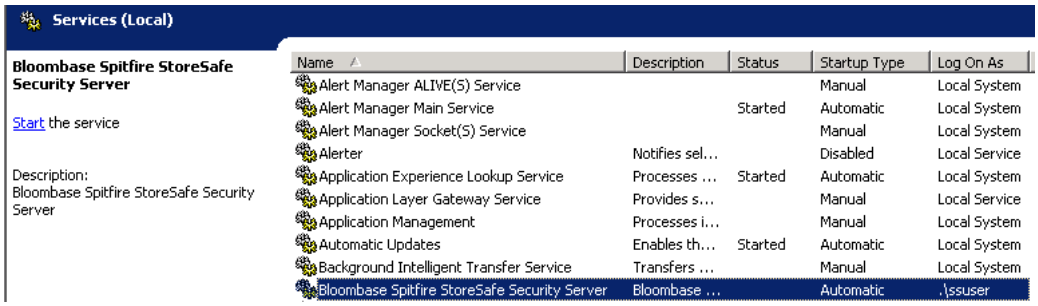
 © 2008 Bloombase, Inc.

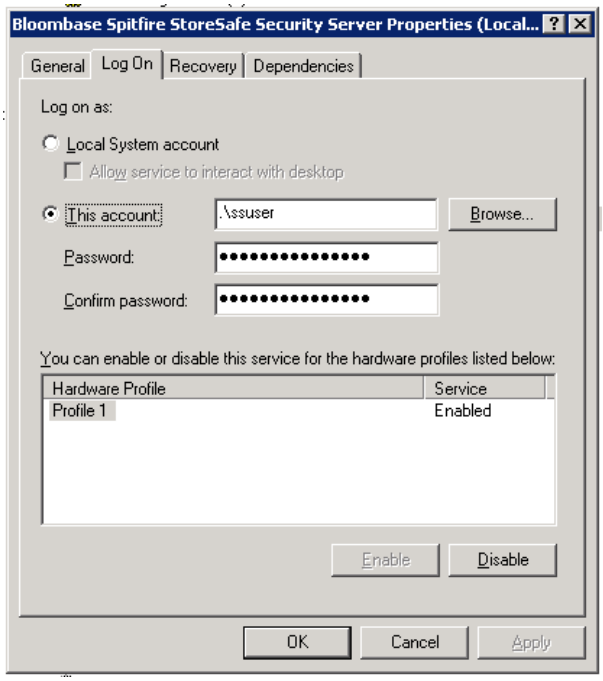
For the storage access control, specify the default user identifier and group identifier to the unmapped id -2 which is used for the mapping between the windows users identifier and the unix user identifiers.

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

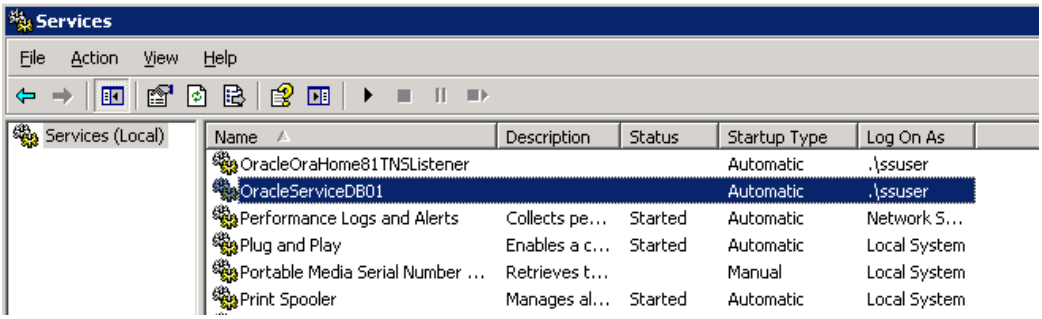


On the Spitfre StoreSafe server machine, change Bloombase Spitfire StoreSafe service to log on as the defined windows user





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

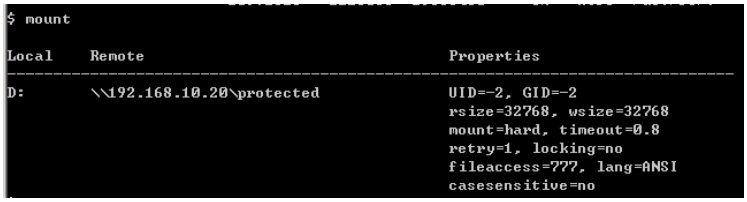


After completed the virtual storage configuration and restarted Spitfire StoreSafe server, connect to the Spitfire StoreSafe virtual storage protected

```
$ 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.

 © 2008 Bloombase, Inc.



Migrate Oracle data files

Encrypt the Oracle data files by copying the file from

```
C:\TEMP
```

to

```
D:
```

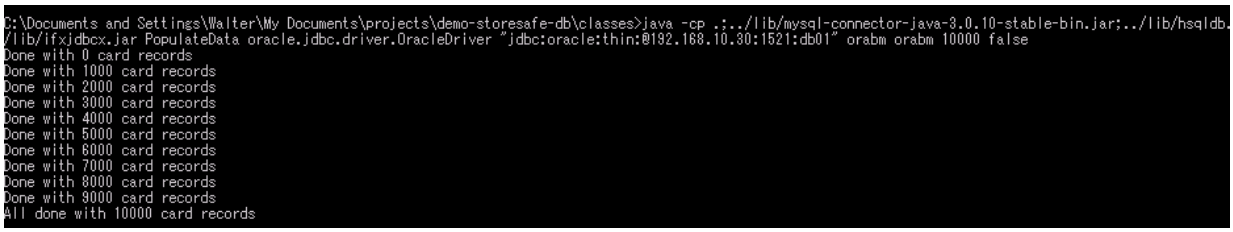
Startup Oracle instance service and listener. With the Oracle data files location unchanged and connected as

```
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.



 © 2008 Bloombase, Inc.

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

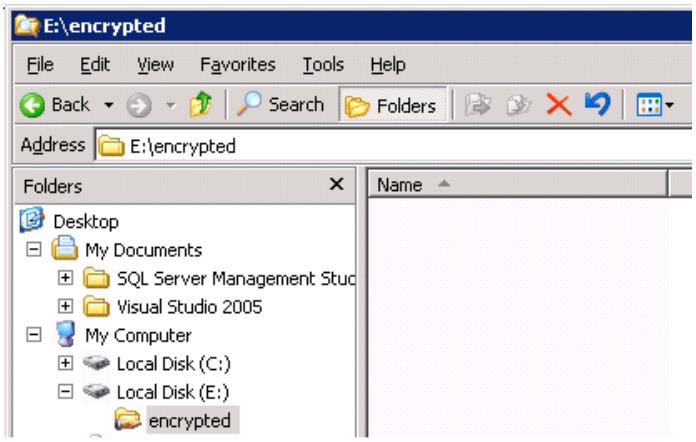
```
E:
```

Create a windows user eg

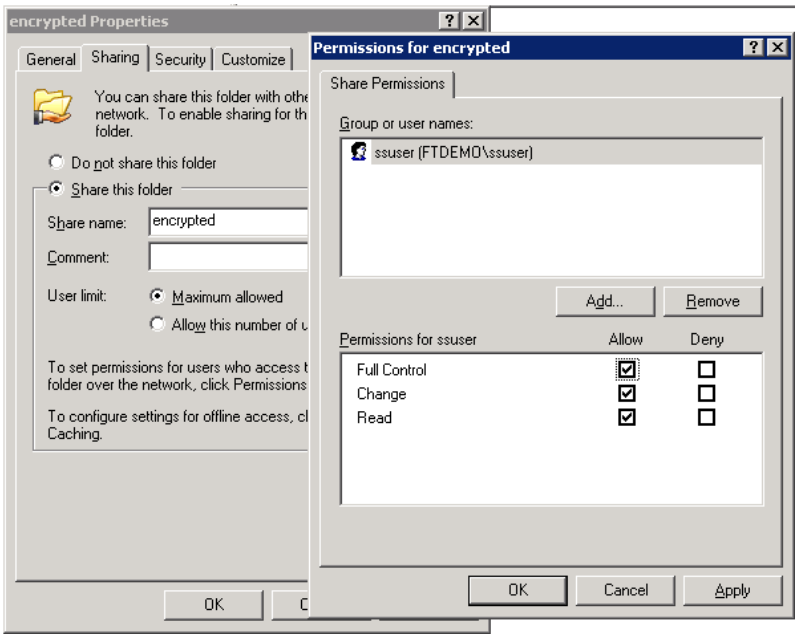
```
ssuser
```

for user connection from Spitfire StoreSafe server.

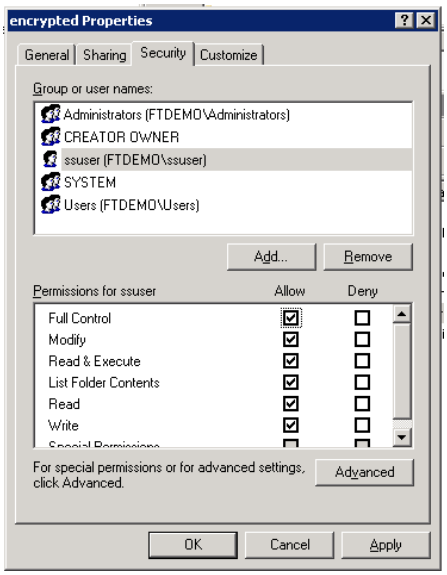
 © 2008 Bloombase, Inc.



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

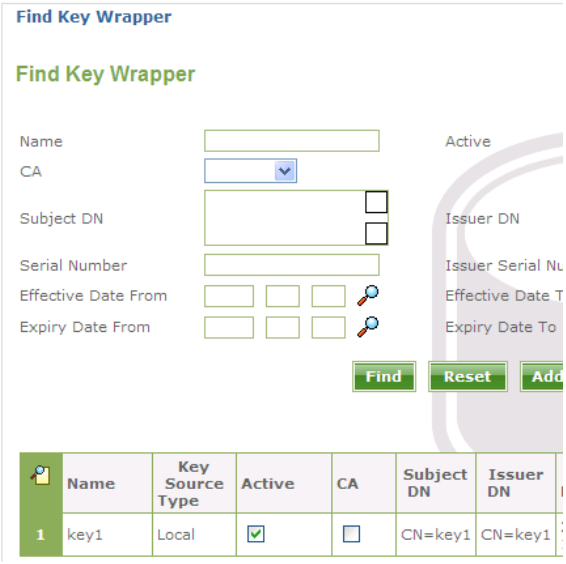


 © 2008 Bloombase, Inc.



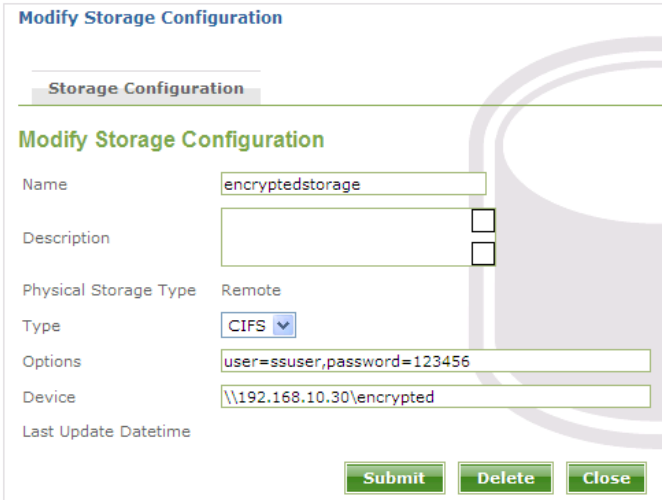
Create Spitfire StoreSafe virtual storage for encryption

Create an encryption key



Create a storage configuration to the encrypted files physical location

 © 2008 Bloombase, Inc.



Create a storage user

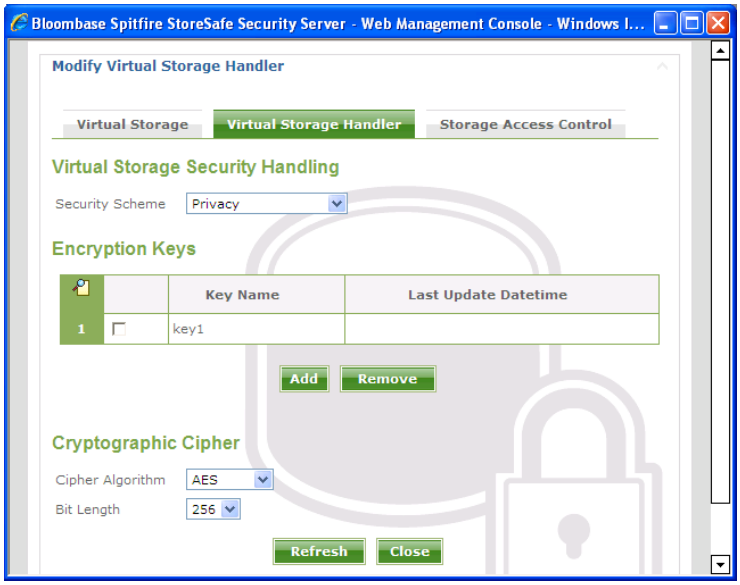
```
ssuser
```

who has the same name as the windows user

Create a virtual storage for the above storage configuration

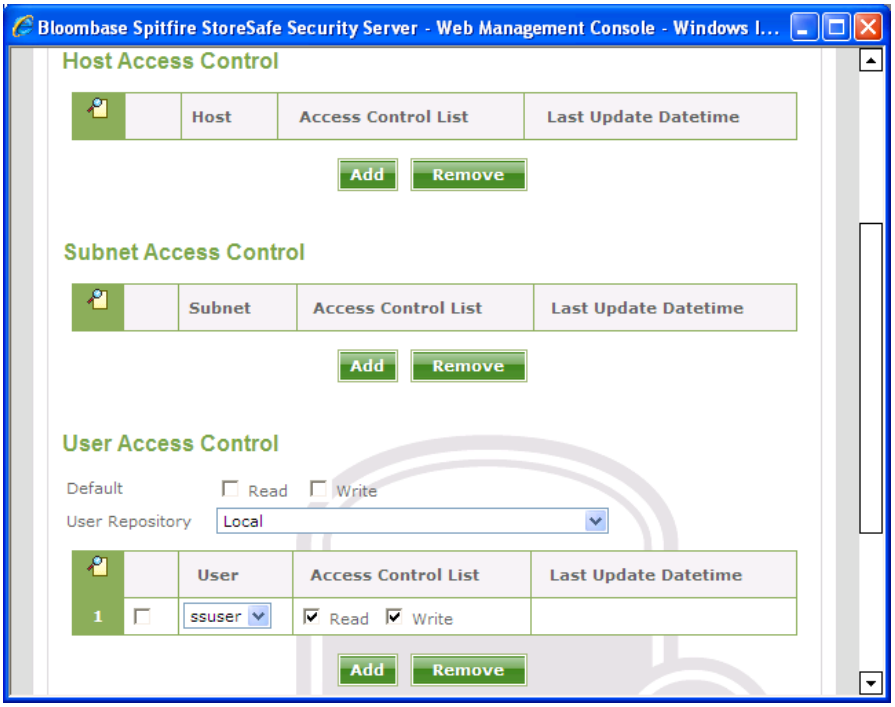
 © 2008 Bloombase, Inc.

Choose the defined encryption key and the appropriate cryptographic cipher

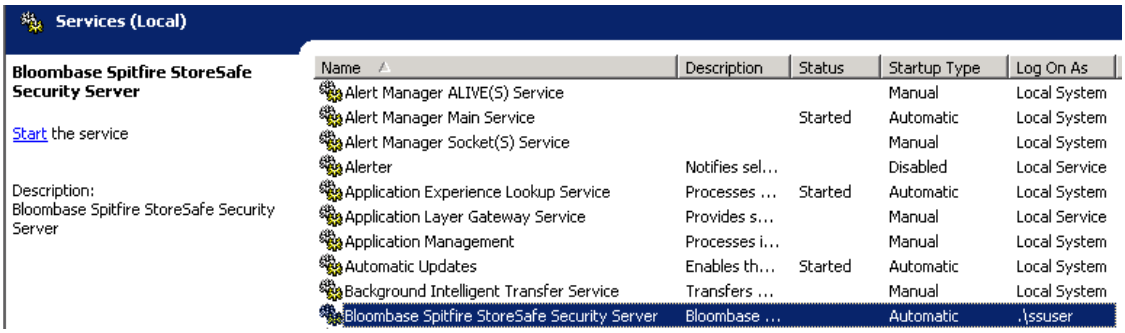


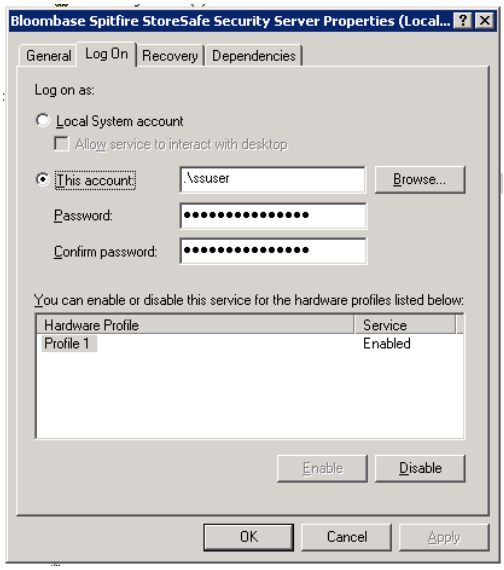
Grant the user access to the defined storage user so that Oracle instance can connect to the Spitfire StoreSafe virtual storage

 © 2008 Bloombase, Inc.

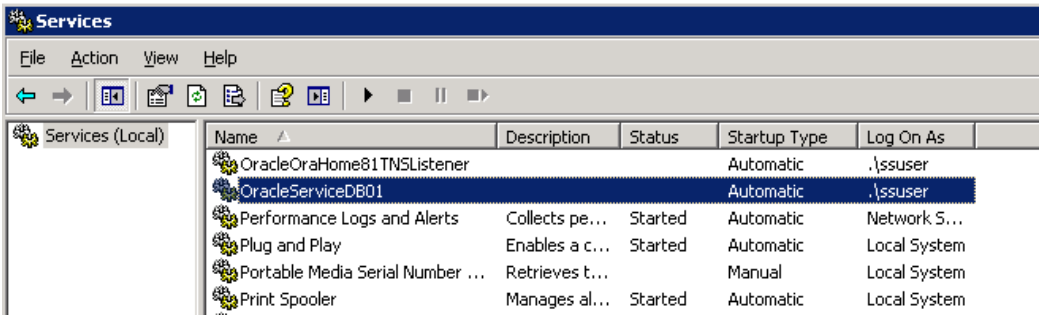


On the Spitfre StoreSafe server machine, change Bloombase Spitfire StoreSafe service to log on as the defined windows user



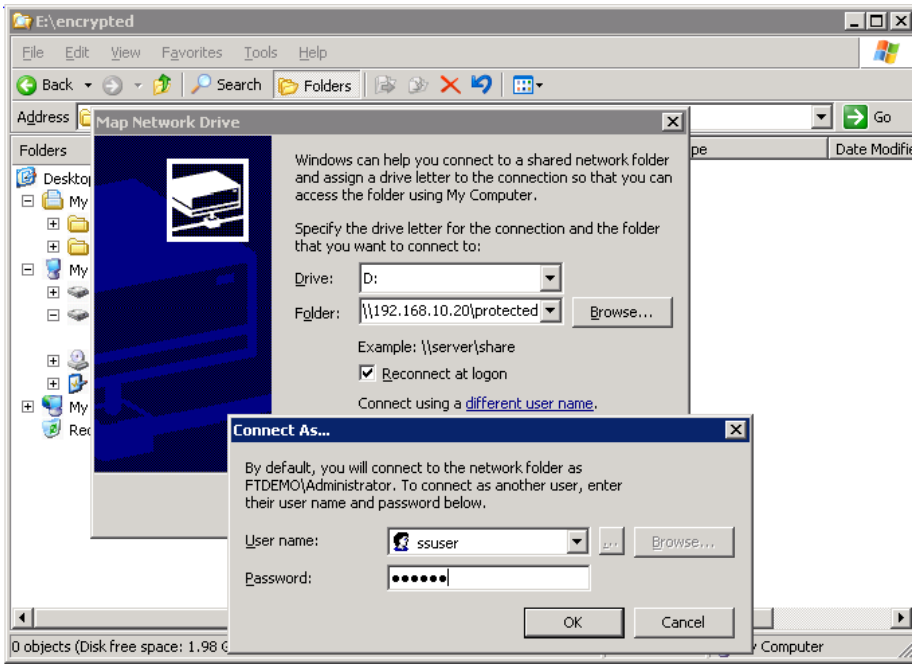


Back to the Oracle server machine, also change the Oracle instance service and Oracle TNS listener to log on as the windows user



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

 © 2008 Bloombase, Inc.



Migrate Oracle data files

Encrypt the Oracle data files by copying the file from

```
C:\TEMP
```

to

```
D:
```

 © 2008 Bloombase, Inc.

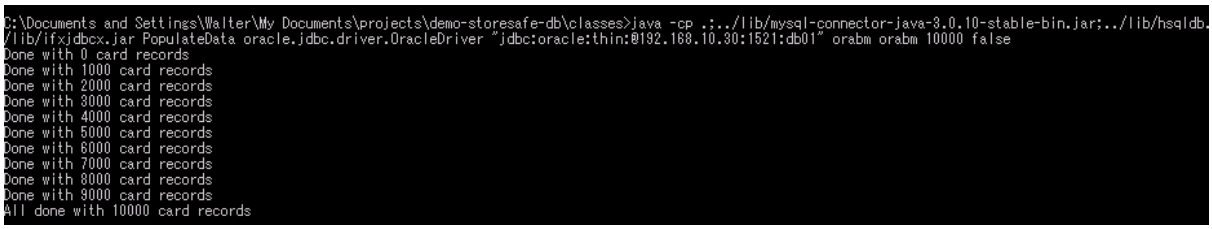
Startup Oracle instance service and listener. With the Oracle data files location unchanged and connected as

```
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.

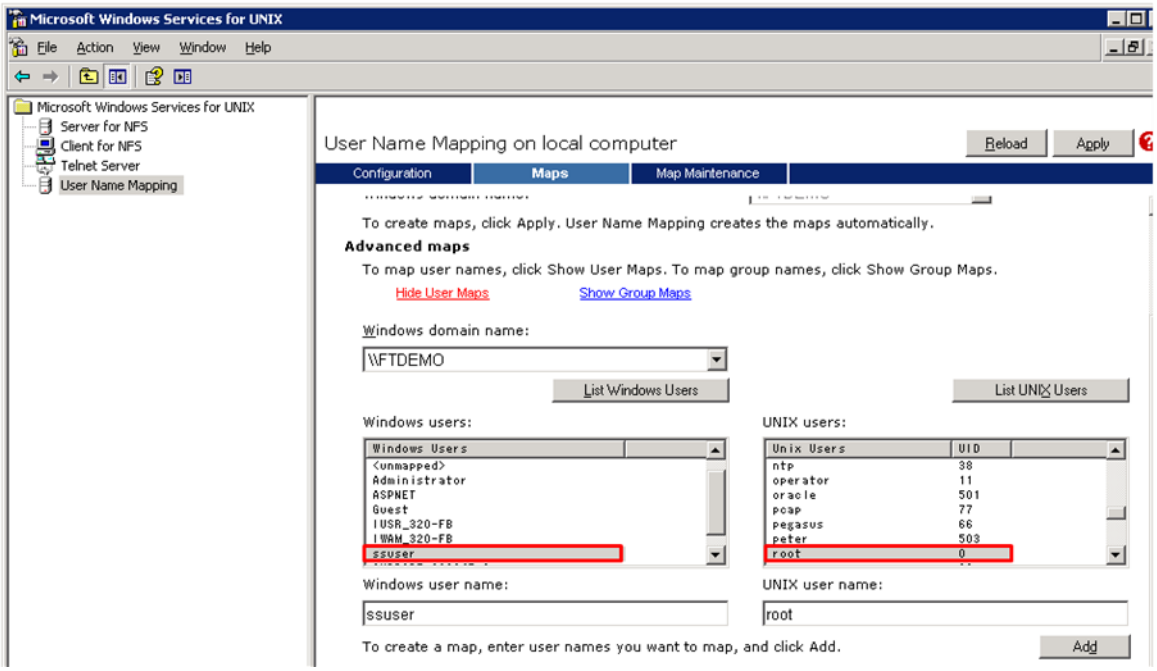


 © 2008 Bloombase, Inc.

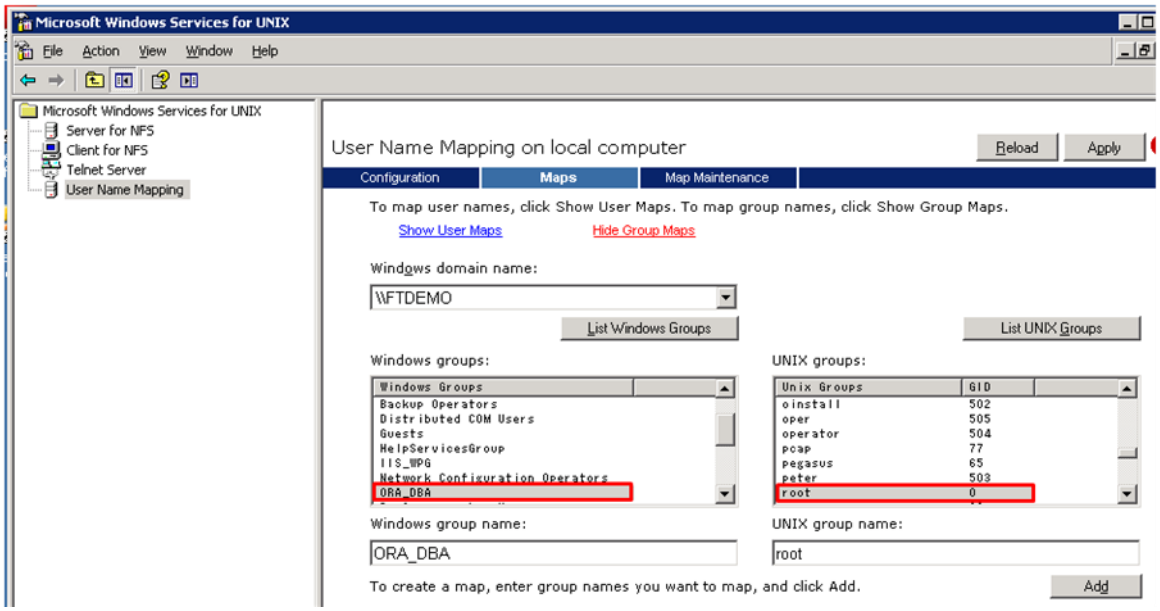
Encryption of Oracle data files by Spitfire StoreSafe on Red Hat Enterprise Linux 4, virtual storage connected by NFS

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 0 and gid of 0 in UNIX.



 © 2008 Bloombase, Inc.



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

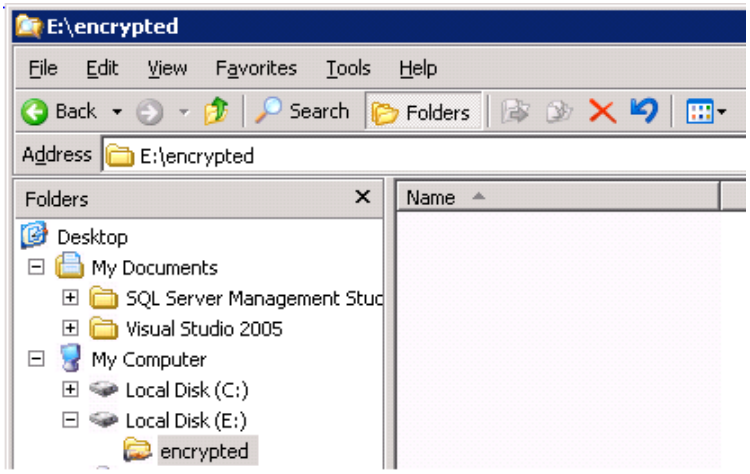
```
E:
```

 © 2008 Bloombase, Inc.

Create a windows user eg

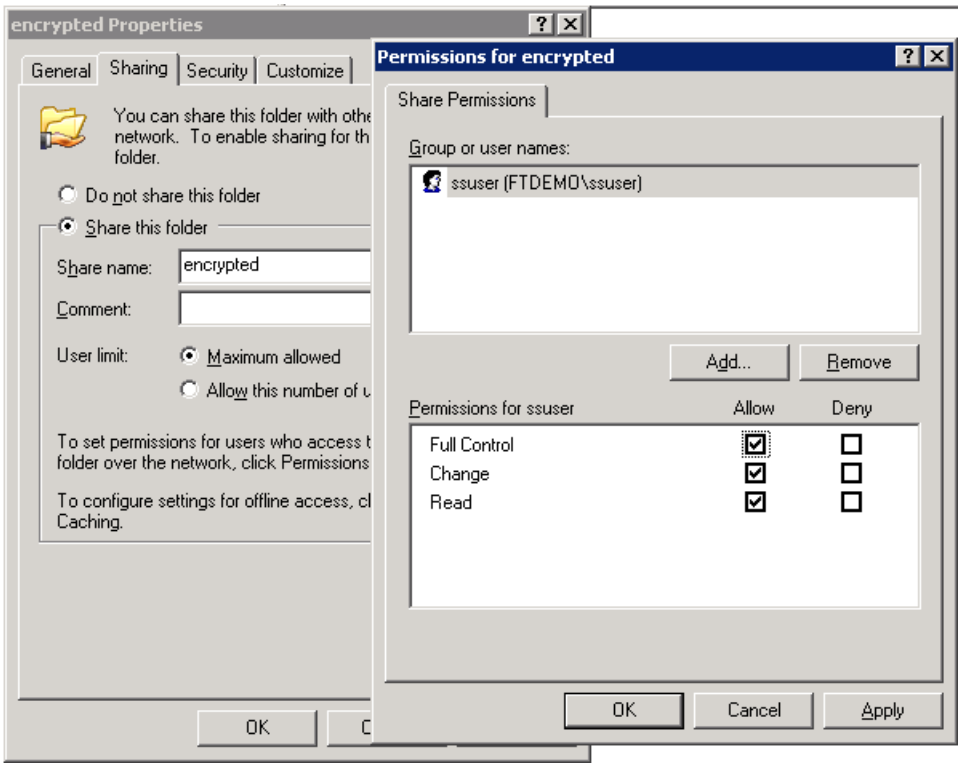
```
ssuser
```

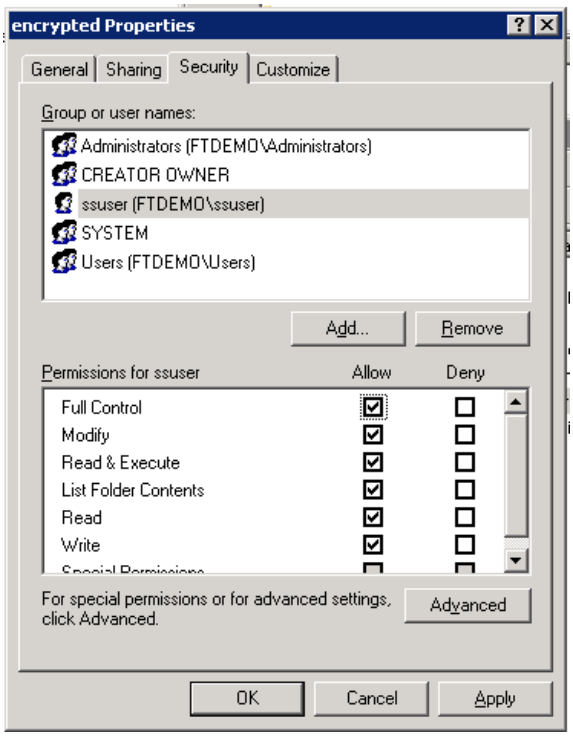
for user connection from Spitfire StoreSafe server.



 © 2008 Bloombase, Inc.

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

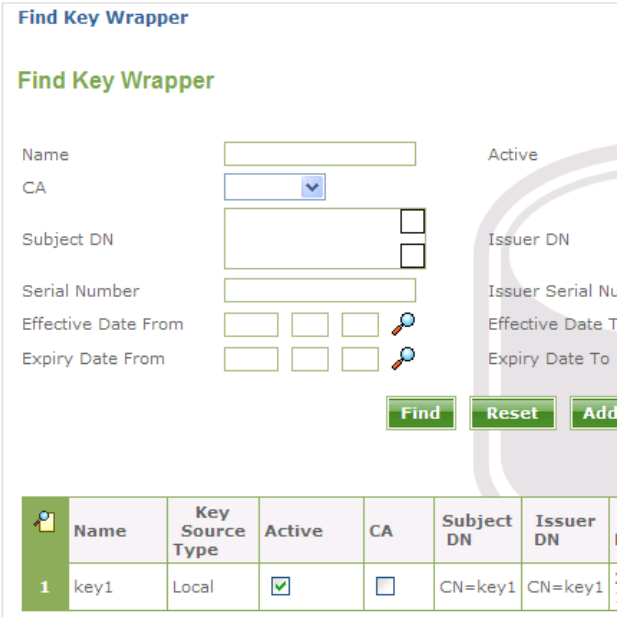




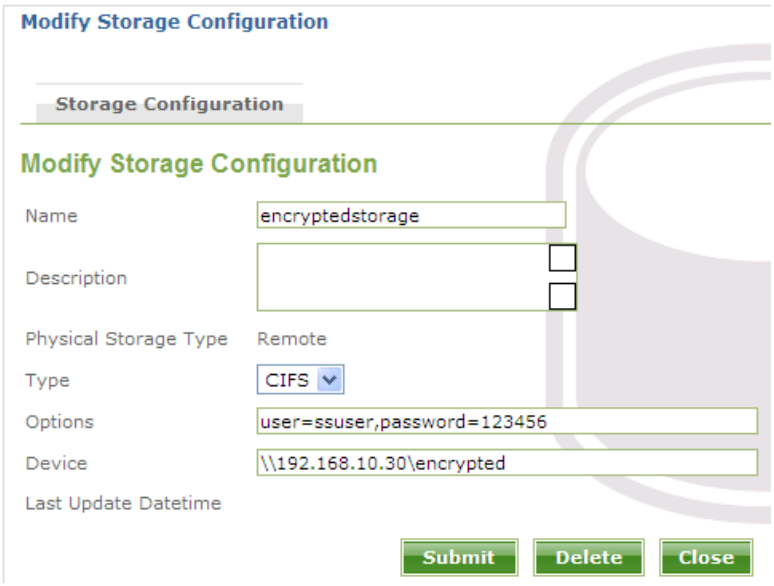
 © 2008 Bloombase, Inc.

Create Spitfire StoreSafe virtual storage for encryption

Create an encryption key



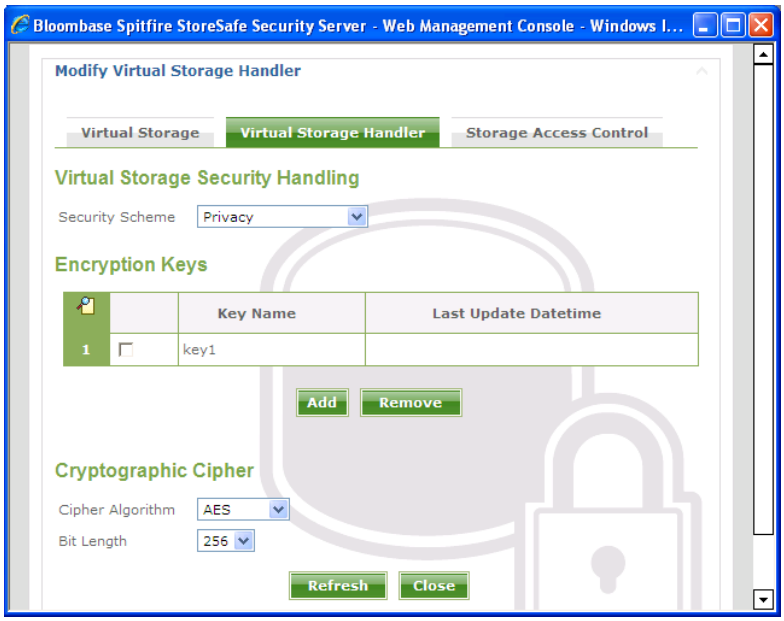
Create a storage configuration to the encrypted files physical location



 © 2008 Bloombase, Inc.

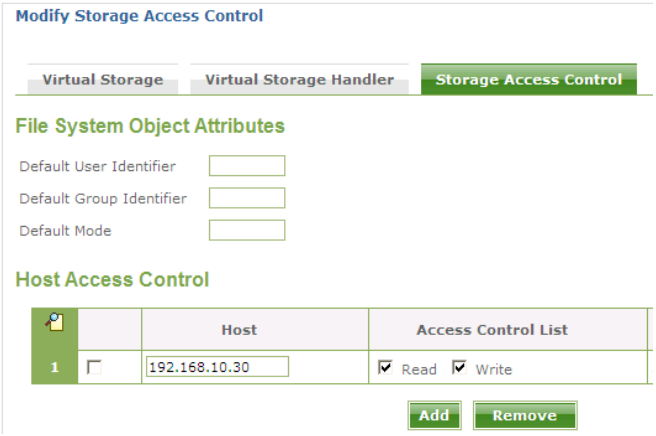
Create a virtual storage for the above storage configuration

Choose the defined encryption key and the appropriate cryptographic cipher

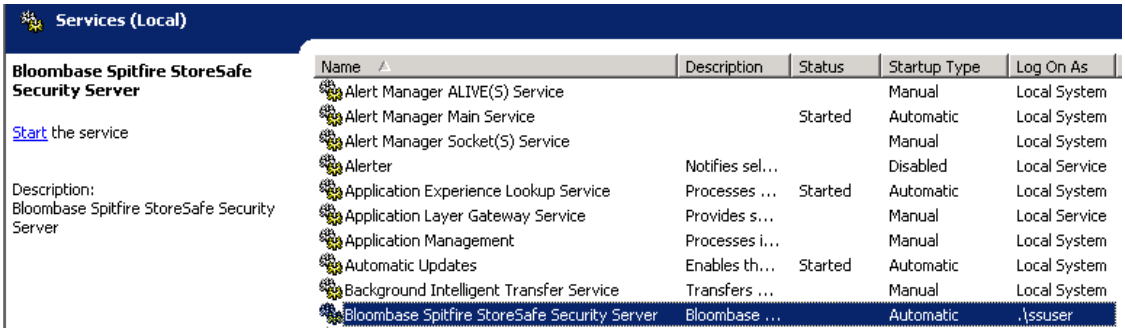


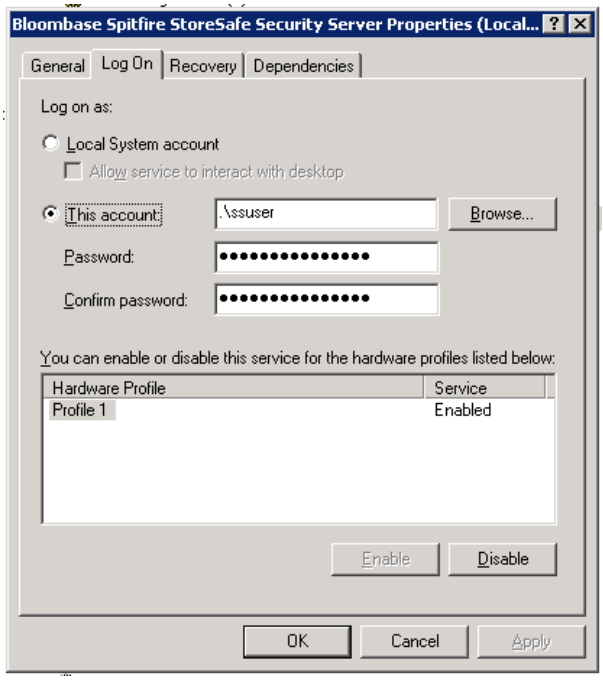
 © 2008 Bloombase, Inc.

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

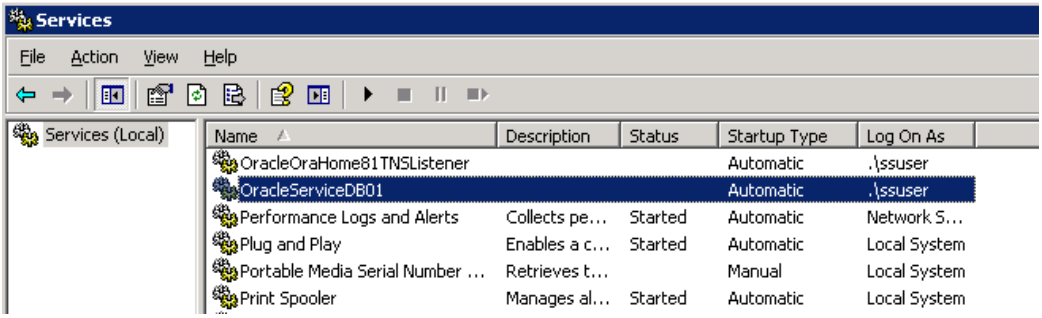




© 2008 Bloombase, Inc.

 © 2008 Bloombase, Inc.

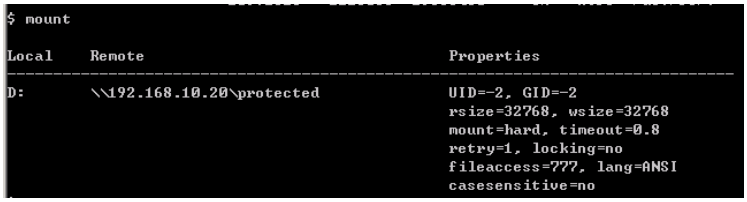
Back to the Oracle server machine, also change the Oracle instance service and Oracle TNS listener to log on as the windows user



After completed the virtual storage configuration and restarted Spitfire StoreSafe server, 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.



Migrate Oracle data files

Encrypt the Oracle data files by copying the file from

```
C:\TEMP
```

to

```
D:
```

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

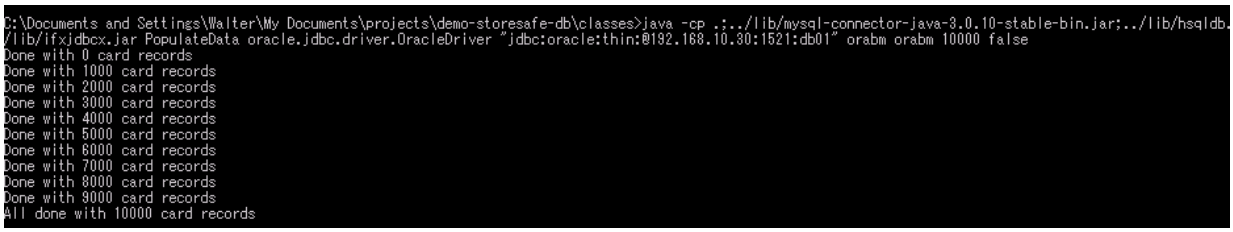
```
D:\ORACLE
```

 © 2008 Bloombase, Inc.

, 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.

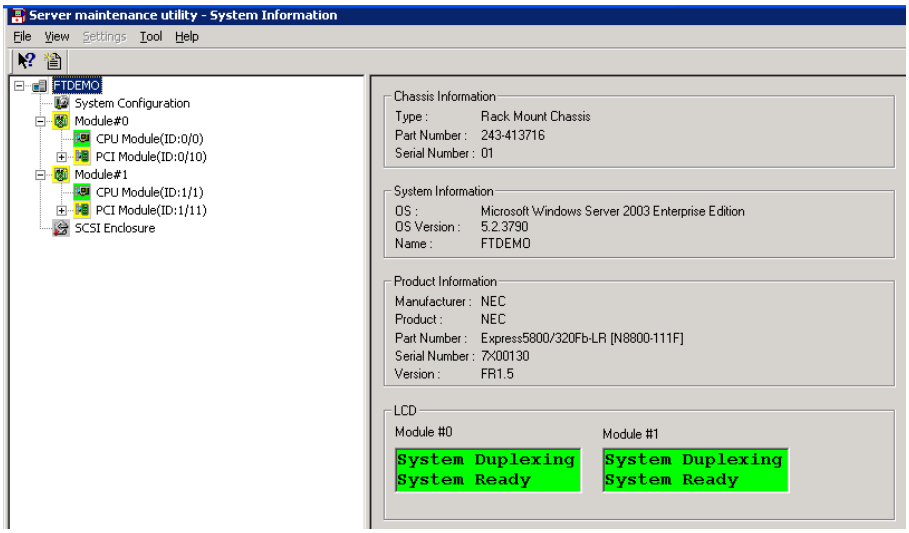


 © 2008 Bloombase, Inc.

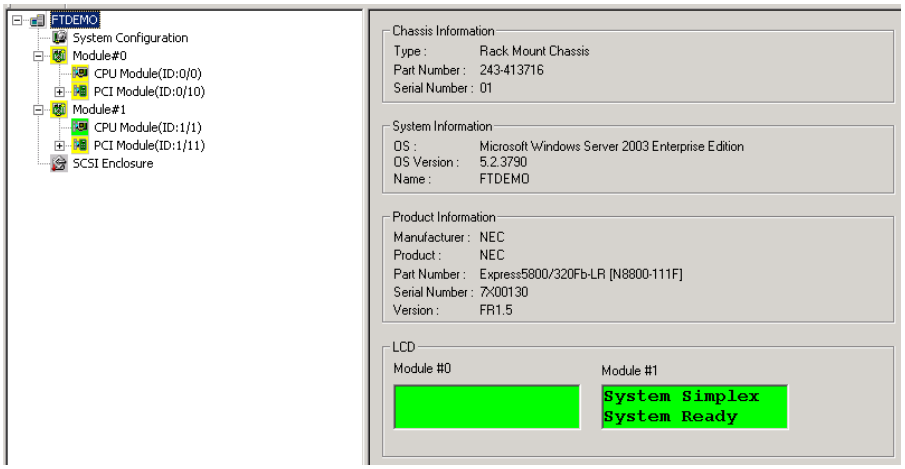
Automatic Failover of Oracle server

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 Expess 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.



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.



 © 2008 Bloombase, Inc.

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.

 © 2008 Bloombase, Inc.

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

 © 2008 Bloombase, Inc.

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.

 © 2008 Bloombase, Inc.

Technical Reference

1. NEC Express5800/ft Fault-Tolerant, http://www.nec.com/global/prod/express/library/brochure/ft_E08FT2.pdf

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

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

4. Bloombase Spitfire StoreSafe Compatibility Matrix for NAS, http://www.bloombase.com/content/8396639C9Q8dkeo46yZ3i7Yvfa6iaCNvwpZ81x