



Interoperability of Bloombase StoreSafe and Thales nShield[®] for Data At- Rest Encryption

June 2015



Executive Summary

Thales nShield Connect enterprise Hardware Security Module (HSM) is validated by Bloombase InteropLab to run with Bloombase StoreSafe data at-rest encryption security solution. This document describes the steps carried out to test interoperability of Thales nShield Connect HSM with Bloombase StoreSafe software appliance on VMware ESXi. Client host systems on Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Oracle Sun Solaris, IBM AIX and HP-UX are tested with Thales powered Bloombase StoreSafe with EMC VNX unified storage system as backend storage.

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, Inc.

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

© 2015 Bloombase, Inc.

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

Thales nShield and Thales keyAuthority are trademarks of Thales, S.A. or its affiliated companies.

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

Document No.: BLBS-TN-Bloombase-StoreSafe-Thales-nShield-Interoperability-USLET-EN-R7

Table of Contents

Table of Contents	3
Purpose and Scope	5
Assumptions	6
Infrastructure	7
Setup	7
Thales Hardware Security Module	9
Bloombase StoreSafe	9
Storage System	9
Client Hosts	9
Configuration Overview	10
Thales nShield	10
Thales Network Configuration	10
Thales nShield Remote File System Setup	11
Thales nShield Client Enrollment	13
Thales Security World Setup	15
EMC VNX Storage	15
Bloombase StoreSafe	17
Thales nShield and Bloombase KeyCastle Integration	18
Encryption Key Provisioning	19
Backend Physical Storage Configuration	22
Secure Storage Configuration	23
Conclusion	27
Disclaimer	29
Acknowledgement	30
Technical Reference	31

Purpose and Scope

This document describes the steps necessary to integrate Thales nShield Connect Hardware Security Module (HSM) with Bloombase StoreSafe to secure sensitive enterprise business persistent data managed in storage systems. Specifically, we cover the following topics:

- Install and configure Bloombase StoreSafe
- Integrate Bloombase StoreSafe with Thales nShield Connect
- Interoperability testing on client host systems including Linux, Windows, IBM AIX, HP-UX and Oracle Sun Solaris

Assumptions

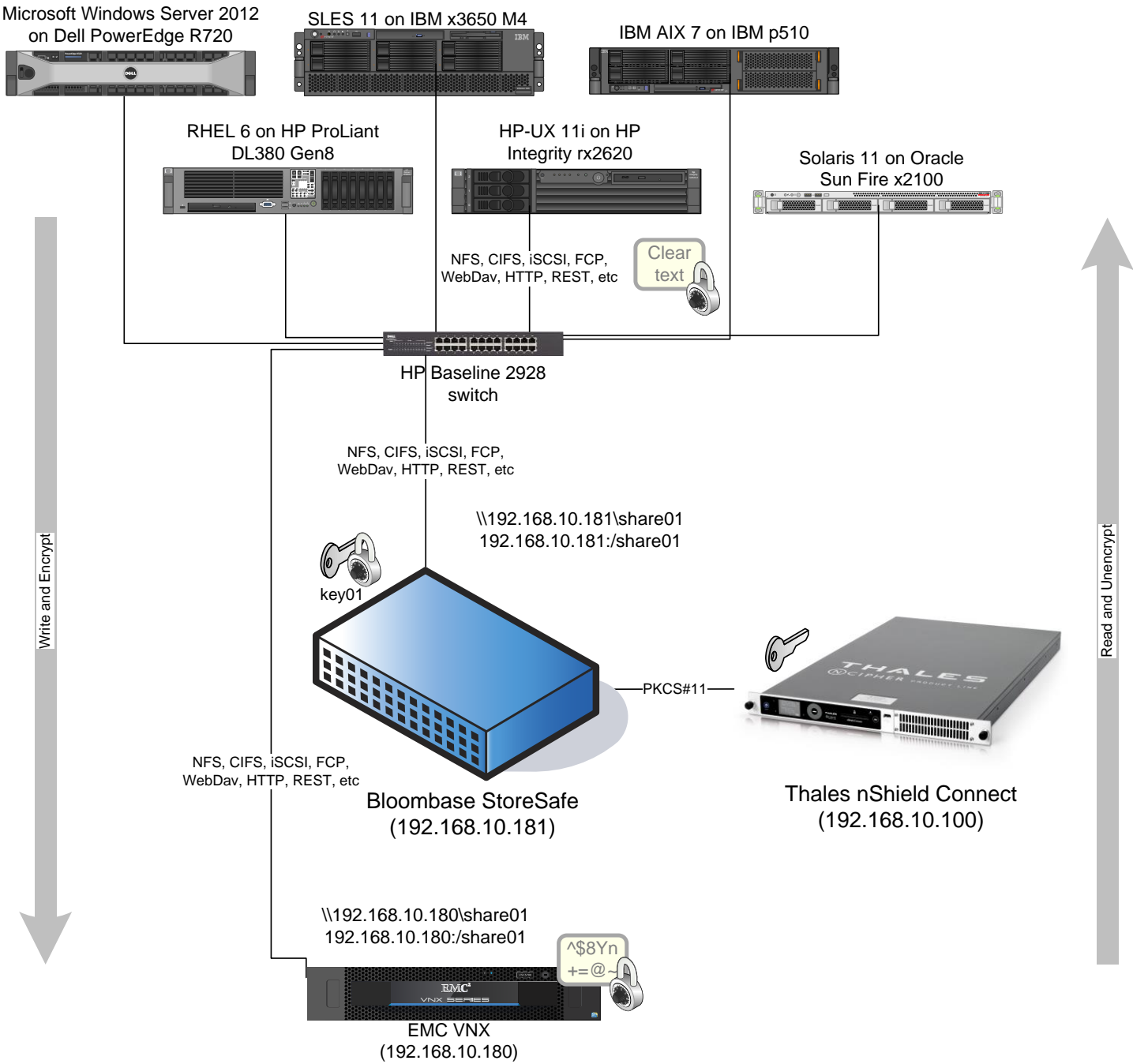
This document describes interoperability testing of Thales nShield with Bloombase StoreSafe. Therefore, it is assumed that you are familiar with operation of Thales nShield, storage systems and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is also assumed that you possess basic UNIX administration skills. The examples provided may require modifications before they are run under your version of operating system.

As Thales nShield is third party hardware option to Bloombase StoreSafe data at-rest encryption security solution, you are recommended to refer to installation and configuration guides of specific model of Thales nShield for your actual use case. We assume you have basic knowledge of storage networking and information cryptography. For specific technical product information of Bloombase 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 diagram



Thales Hardware Security Module

PKCS#11 Hardware Security Module	Thales nShield Connect
----------------------------------	------------------------

Bloomberg StoreSafe

Bloomberg StoreSafe	Bloomberg StoreSafe Software Appliance v3.4 on Bloomberg OS 5 (security hardened Linux OS kernel version 2.6)
nShield Client Security World Software Package	nCSS v11.70 Security World Software for Linux 64-bit
FIPS Mode	Non-strict FIPS security world
Server	VMware Virtual Machine (VM) on VMware ESXi 5.5
Processor	4 x Virtual CPU (vCPU)
Memory	8 GB

Storage System

Storage System	EMC VNX Virtual Appliance on ESXi 5.5
----------------	---------------------------------------

Client Hosts

Model	Dell PowerEdge R720	HP ProLiant DL380 Gen8	IBM System x3650 M4	HP Integrity rx2620	IBM System p5 510	Oracle Sun Fire x2100
Operating System	Microsoft Windows Server 2012	Red Hat Enterprise Linux 6	SUSE Linux Enterprise 11	HP-UX 11i	IBM AIX 7	Oracle Solaris 11

Configuration Overview

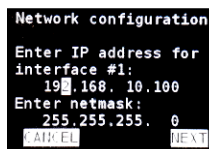
Thales nShield

The following operations can be performed by any user in the nFast group. Administrator access is needed for stopping and starting the hardserver. First install the Security World Software for Linux 64-bit.

After installation of the Security World Software is complete, the HSM can be configured.

Thales Network Configuration

The Thales nShield Connect is installed with network settings provisioned. In this interoperability test, the Thales nShield Connect is assigned with IP address 192.168.10.100.



Thales nShield Remote File System Setup

In this interoperability test effort, Bloombase StoreSafe serves as client of Thales nShield Connect as well as the Remote File System (RFS) of Thales Security World.

Thales nShield Support Software (nCSS) for Linux is installed at Bloombase OS by switching on maintenance mode and signing in to the command line interface (CLI) console.

```
[root@ss_nshield ~]# cd /opt/nfast/bin/
```

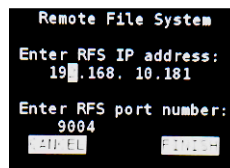
Configuration data (ESN and kneti hash) for RFS setup is acquired from Thales nShield Connect.

```
[root@ss_nshield bin]# ./anonkneti 192.168.10.100
```

Bloombase StoreSafe is provisioned as the Remote File System (RFS) for Thales Security World.

```
[root@ss_nshield bin]# ./rfs-setup 192.168.10.100 4F14-106E-6B49 188c50ee38c0f0453c1653955f78385d698c9e28
```

Remote File System (RFS) is configured and set to Bloombase StoreSafe instance.



Optionally, you may want to permit module config files on the RFS to be modified and then loaded to the module by turning on the **auto push** option (from menu 1-1-6-2):

- a. Select **On**.
- b. Enter the IP address of the RFS.
- c. Select **Continue**.

Then configure log file storage (from menu 1-1-7) by selecting one of the following options:

- **Append**: stores the files on the module and RFS OR
- **Log**: stores the files on the module only.

Finally, set the time and date on the module as UTC (from menu 1-1-8) and then reboot the module.

Once the Thales HSM comes up, to verify if basic configuration is all set, execute “enquiry” command at Bloombase command line interface (CLI) console in maintenance mode.

```

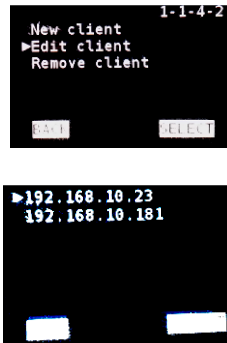
[root@ss_nshield bin]# ./enquiry
Server:
enquiry reply flags  none
enquiry reply level  Six
serial number        4F14-106E-6B49
mode                 operational
version              2.71.2
speed index          544
rec. queue           442..642
level one flags      Hardware HasTokens
version string       2.71.2cam2, 2.50.16cam18 built on Sep 23 2010 20:40:16, 2.
59.6cam1
checked in           00000000487debd5 Wed Jul 16 20:38:45 2008
level two flags      none
max. write size      8192
level three flags    KeyStorage
level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasP
ollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp Ha
sPCIPush HasKernelInterface HasLongJobs ServerHasLongJobs AESModuleKeys NTokenCm
ds JobFragmentation LongJobsPreferred Type2Smartcard ServerHasCreateClient HasIn
itiliseUnitEx
module type code     0
product name         nFast server
device name
EnquirySix version   4
impath kx groups
feature ctrl flags   none
features enabled     none
version serial       0
remote server port   9004

Module #1:
enquiry reply flags  UnprivOnly
enquiry reply level  Six
serial number        4F14-106E-6B49
mode                 operational
version              2.50.16
speed index          544
rec. queue           9..152
level one flags      Hardware HasTokens
version string       2.50.16cam18 built on Sep 23 2010 20:40:16, 2.59.6cam1
checked in           000000004856847b Mon Jun 16 23:19:23 2008
level two flags      none
max. write size      8192
level three flags    KeyStorage
level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasP
ollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp Ha
sPCIPush HasKernelInterface HasLongJobs ServerHasLongJobs AESModuleKeys NTokenCm
ds JobFragmentation LongJobsPreferred Type2Smartcard ServerHasCreateClient HasIn
itiliseUnitEx
module type code     7
product name         nC1003P/nC3023P/nC3033P
device name         Rt1
EnquirySix version   6
impath kx groups     DHPrime1024 DHPrime3072
feature ctrl flags    LongTerm
features enabled      StandardKM
version serial       25
connection status     OK
connection info       esn = 4F14-106E-6B49; addr = INET/192.168.10.100/9004; ku
hash = ecf2e3e7c92fa6427b5b09102a846fa0d489eed2, mech = Any; time-limit = 24h; d
ata-limit = 8MB
max exported modules  10
rec. LongJobs queue   8
SEE machine type      PowerPCSXF
supported KML types   DSAp1024s160 DSAp3072s256
using impath kx grp   DHPrime3072

```

Thales nShield Client Enrollment

Once RFS configuration is done, the Thales nShield Connect needs to allow access from Bloombase StoreSafe instance with IP address 192.168.10.181. This is done using the Connect front panel option for New Client (menu 1-1-4-1)



Once RFS configuration is done, Bloombase software appliance then needs to be registered as the HSM client by nCSS enroll utility.

```
[root@ss_nshield bin]# ./nethsmenroll 192.168.10.100
```

Thales RFS synchronization of clients is configured at Bloombase StoreSafe instance. Run this command on the RFS for every client IP address.

```
[root@ss_nshield bin]# ./rfs-setup --gang-client --write-noauth 192.168.10.181
```

Thales client synchronization of RFS is configured at Bloombase StoreSafe instance. Run this command on each client to connect to RFS.

```
[root@ss_nshield bin]# ./rfs-sync --setup --no-authenticate 192.168.10.181
```

If you have multiple HSMs to be used in high-availability mode, create the cknfastrc file in the \$NFAST_HOME (typically /opt/nfast/) directory, with the entry:

```
CKNFAST_LOADSHARING=1
```

Please note that if using OCS protection, only 1-of-N persistent cardset is supported. You must have an operator card inserted into every slot from the same 1-of-N card set, at the time of application startup. This setup was tested with this 1-of-N configuration. However, if you want to use K-of-N OCS cardset, you may be able to use Thales provided 'preload' utility for loading keys on a particular slot. Please refer to Thales Connect User guide for details.

Run command

```
/opt/nfast/bin/ckcheckinst
```

as the sanity check for if everything is working on the HSM and PKCS#11 layer.

```

[root@bloomberg02 bin]# ./ckcheckinst
PKCS#11 library interface version 2.01
        flags 0
        manufacturerID "nCipher Corp. Ltd"
        libraryDescription "nCipher PKCS#11 1.95.1"
        implementation version 1.95

Slot  Status          Label
====  =====
      0  Fixed token    "accelerator"
      1  Operator card  "demo-ocs-cardset"

Select slot number to run library test or 'R'etry or to 'E'xit: 1
Using slot number 1.

Please enter the passphrase for this token (No echo set).
Passphrase:

Test                               Pass/Failed
----                               -
1 Generate RSA key pair            Pass
2 Generate DSA key pair            Pass
3 Encryption/Decryption            Pass
4 Signing/Verification             Pass

Deleting test keys                  ok

PKCS#11 library test successful.

```

In this interoperability test, Slot 1 has been used for key protection with the HSM as shown in the following entries in Bloomberg StoreSafe

```
pkcs11-nfast.properties
```

configuration file:

```

name=nfast
library=/opt/nfast/toolkits/pkcs11/libcknfast.so
attributes=compatibility
slotListIndex=1

```

The HSM key protection will typically be an Operator Card Set (OCS) (as shown in the output above), but can alternatively be a softcard.

HSM PKCS#11 integration uses standard SunPKCS11 provider. This makes selection of slot customer configurable. This can optionally be reconfigured, by modifying

```
slotListIndex
```

entry in Bloomberg StoreSafe

```
pkcs11-nfast.properties
```

property file.

Please refer to “nShield Connect User Guide” for detailed setup and configurations.

Thales Security World Setup

Thales Security World is then initialized and set up.

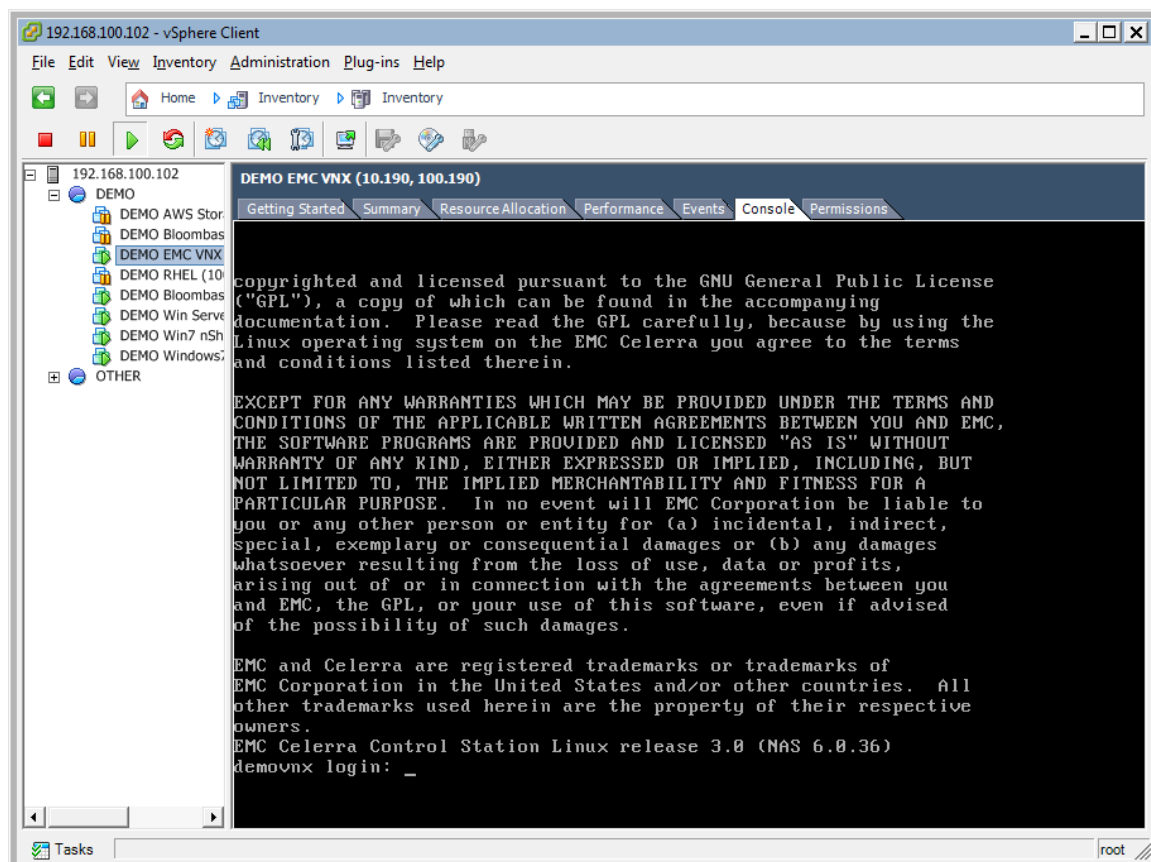


Please refer to “nShield Connect User Guide” for detailed setup and available configuration options.

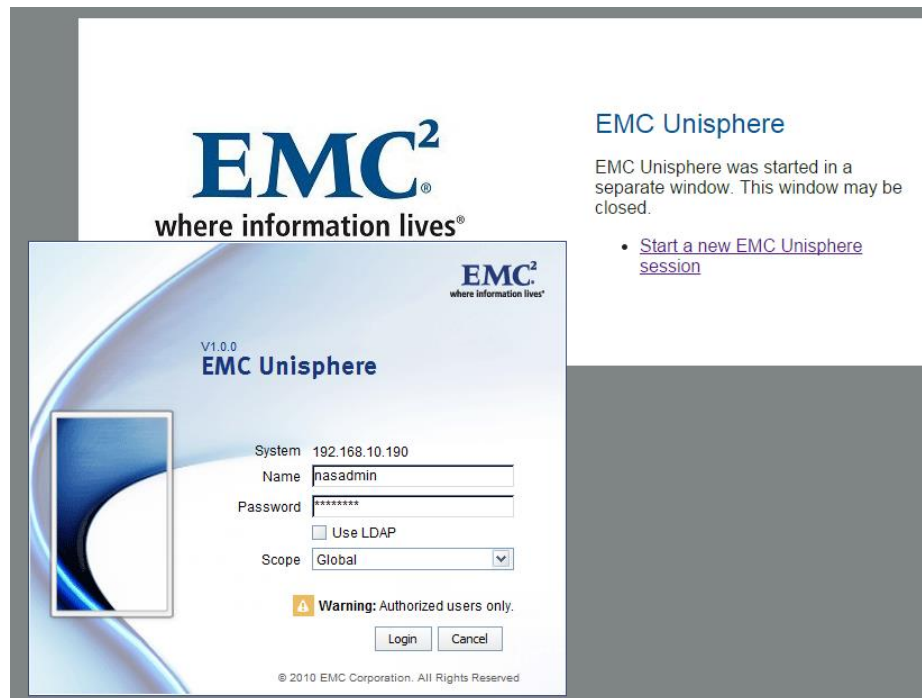
Note: the previous operations can be performed by any user in the nFast group; however, administrator access is needed for stopping and starting the hardware.

EMC VNX Storage

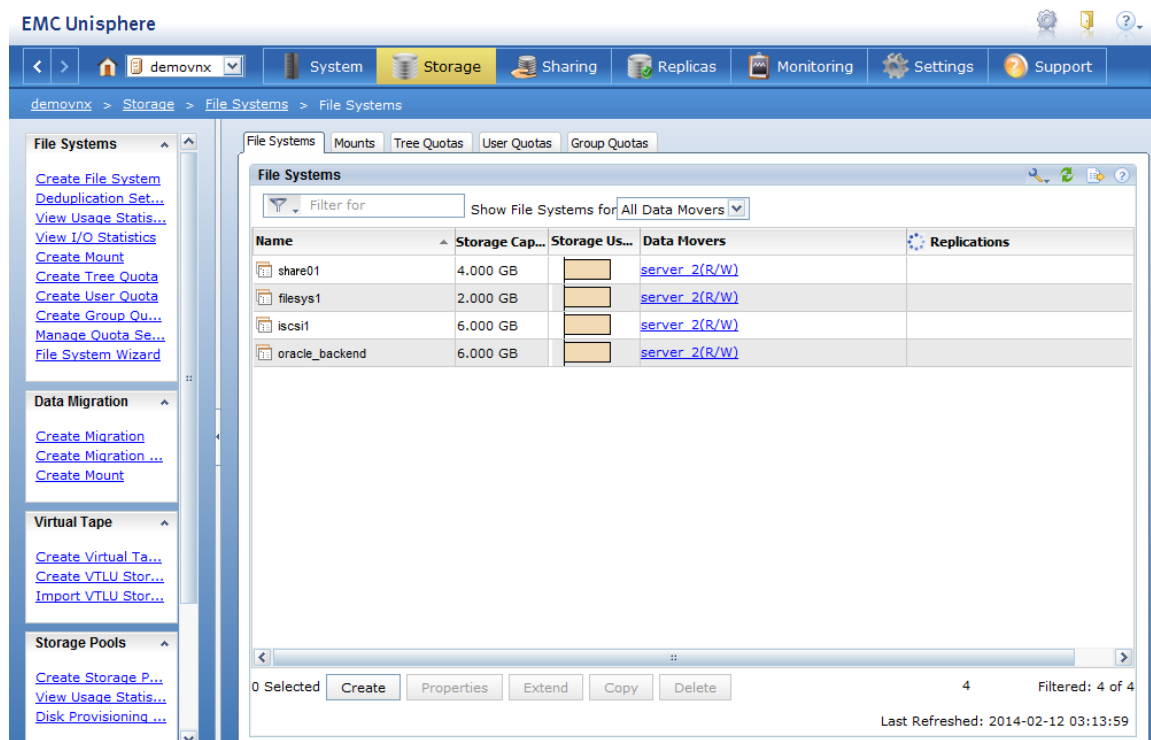
EMC VNX virtual appliance is used in this interoperability test which is able to provide storage services over network storage protocols including NFS, CIFS, iSCSI, etc.



EMC VNX is a unified storage system supporting multiple network storage protocols including NFS, CIFS, HTTP, FCP, FCoE, iSCSI, etc.

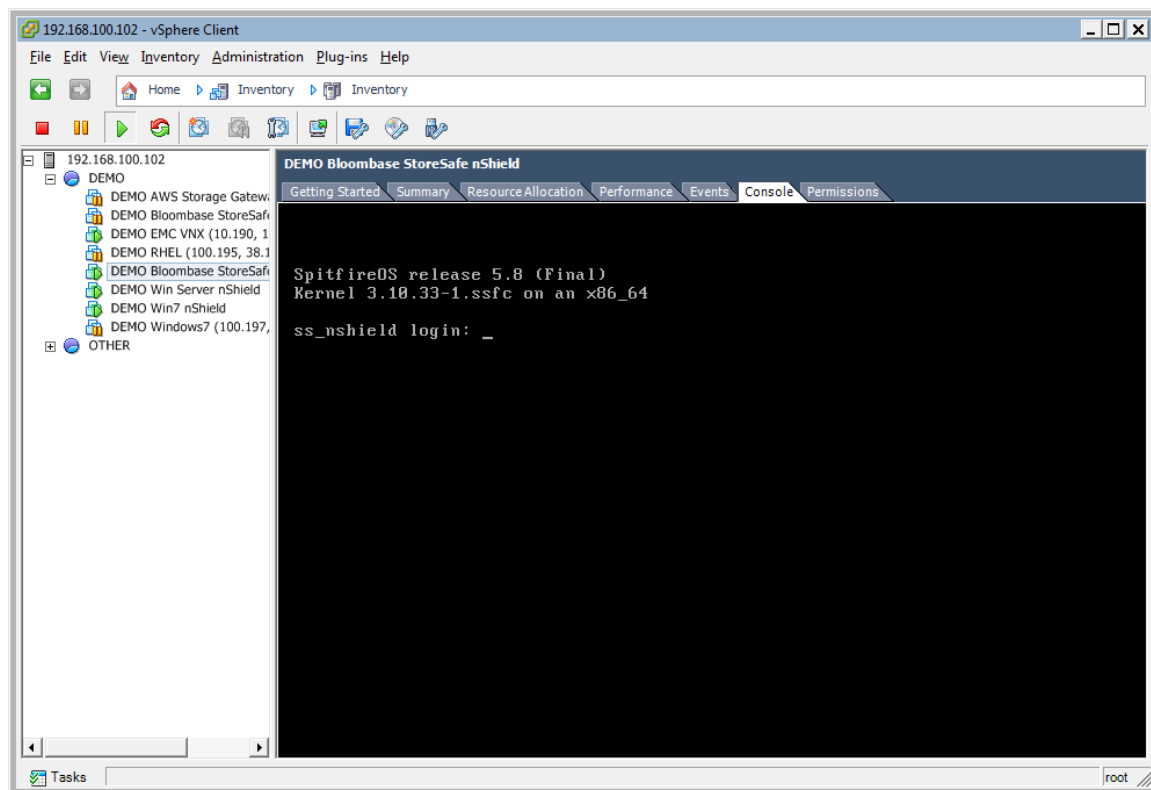


CIFS and NFS storage resources are provisioned on EMC VNX to be used in this testing.

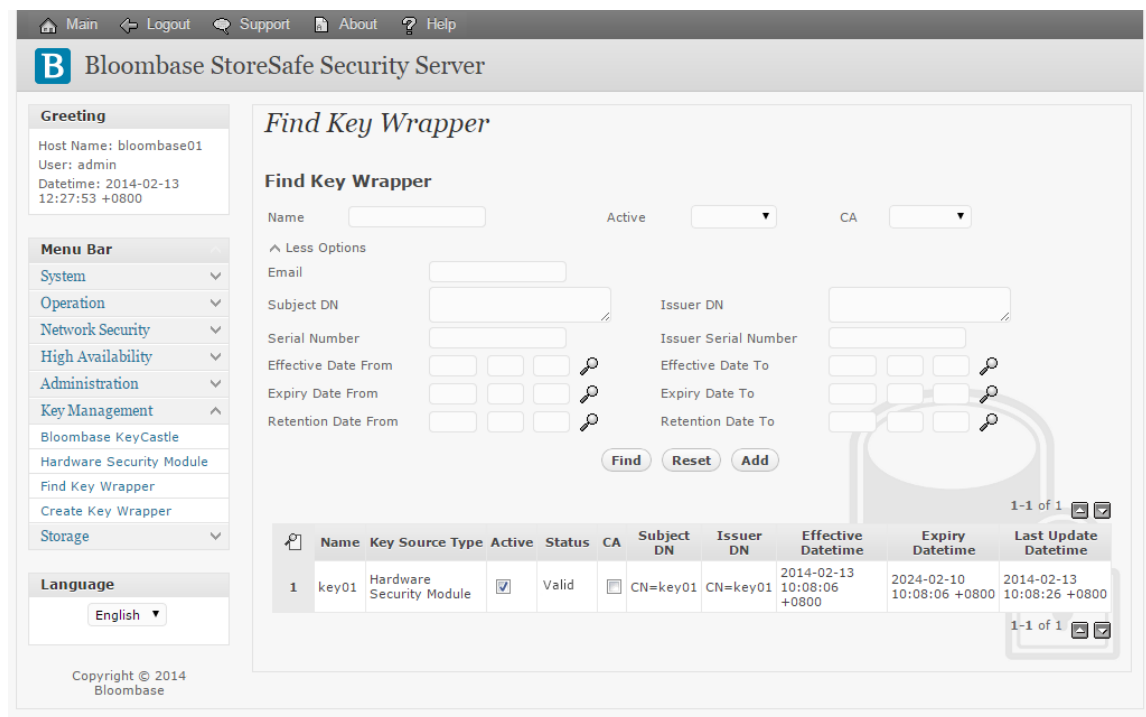


Bloombase StoreSafe

Bloombase StoreSafe delivers unified data at-rest encryption security of files, block devices, objects, sequential storages, etc. In this interoperability test, file-based encryption security service is validated against Bloombase StoreSafe with keys managed at Thales nShield Connect HSM.



Bloombase StoreSafe software appliance is deployed as a virtual appliance (VA) on VMware ESXi.



Thales nShield and Bloombase KeyCastle Integration

To enable the built-in Bloombase KeyCastle to utilize keys in the network attached Thales nShield Connect HSM. The hardware security module configuration at Bloombase web management console has to be set up.

Bloombase supports Thales nShield out of the box. When a Thales nShield is configured at Bloombase web management console, select Module as 'nfast' which allows embedded Bloombase KeyCastle module to utilize Thales nFast driver to access Thales nShield Connect HSM over standard PKCS#11 protocol.

In this scenario, the Thales nShield Connect HSM is assigned a token label namely 'nShield'. Again, the use of slot is customer configurable. This can optionally be reconfigured, by modifying

```
slotListIndex
```

entry in Bloombase StoreSafe

```
pkcs11-nfast.properties
```

property file.

When prompted for pins, plug in nShield OCS card at nShield Connect HSM and enter nShield OCS card pin.

Modify Hardware Security Module

Modify Hardware Security Module

Module

Label

Pin

Confirm Pin

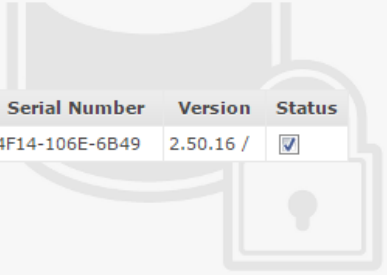


When Thales nShield HSM resource is properly provisioned at Bloombase StoreSafe, the status would show up as 'Active'.

List Hardware Security Module

List Hardware Security Module

	Label	Present	Slot	Token	Module	Manufacturer	Model	Serial Number	Version	Status
1	nShield	<input checked="" type="checkbox"/>		1	nfast	Thales	544	4F14-106E-6B49	2.50.16 /	<input checked="" type="checkbox"/>



Encryption Key Provisioning


Generate encryption key with name 'key01' in bundled Bloombase KeyCastle key life-cycle management tool

Modify Key Wrapper

Key Wrapper Upload Key Contents Modify Key Source CRLDP OCSF Permissions

Modify Key Wrapper

Name	<input type="text" value="key01"/>
Type	Asymmetric
Active	<input checked="" type="checkbox"/>
Exportable	<input type="checkbox"/>
Key Bit Length	2048 ▼
Signature Hash	SHA256 ▼
Key Usage	<input type="checkbox"/> Digital Signature
	<input type="checkbox"/> Non Repudiation
	<input type="checkbox"/> Key Encipherment
	<input type="checkbox"/> Data Encipherment
	<input type="checkbox"/> Key Agreement
	<input type="checkbox"/> Key Cert Sign
	<input type="checkbox"/> C R L Sign
	<input type="checkbox"/> Encipher Only
	<input type="checkbox"/> Decipher Only
Extended Key Usage	<input type="button" value="Add"/> <input type="button" value="Remove"/>
Owner	admin
Last Update Datetime	



To generate key in attached Thales nShield Connect HSM, select Key Source Type as “Hardware Security Module”, Module as “nfast” and the assigned HSM token label, in this case “nShield”. Ensure you import a key from the HSM before you submit the key wrapper.

When prompted for pin, plug in nShield OCS card at nShield Connect HSM and enter nShield OCS card pin.

Modify Key Source

Key Wrapper **Modify Key Source** **Permissions**

Modify Key Source

Type

Hardware Security Module

Module

Token

Alias

Pin

Confirm Pin



Or if key already exists, simply choose from the pull down box.

Modify Key Source

Key Wrapper

Modify Key Source

Permissions

Modify Key Source

Type Hardware Security Module ▼

Hardware Security Module

Module nfast ▼

Token nShield ▼

Key key01 ▼

Refresh

Add Key

Submit

Close



Backend Physical Storage Configuration

Physical storage namely 'share01' is configured to be secured by Bloombase StoreSafe using encryption.

Modify Storage Configuration

Physical Storage**Permissions**

Physical Storage Configuration

Name	share01
Description	
Physical Storage Type	Remote ▼
Type	Common Internet File System (CIFS) ▼
Host	192.168.10.180
Share Name	share01
Read Size	
Write Size	
Synchronous	<input type="checkbox"/>
Mount Hard	<input type="checkbox"/>
User	Administrator
Password	
Options	
Owner	admin
Last Update Datetime	2014-02-13 10:07:40 +0800

Submit**Delete****Close**



Secure Storage Configuration

Virtual storage namely 'share01' of type 'File' is created to virtualize physical storage 'share01' for application transparent encryption protection over network file protocols including CIFS and NFS.

Modify Virtual Storage

Virtual Storage Protection Access Control Permissions

Modify Virtual Storage

Name	share01
Status	<input checked="" type="checkbox"/>
Description	
Active	<input checked="" type="checkbox"/>
Mode	File
Owner	admin
Last Update Datetime	2014-02-13 10:09:11 +0800

Settings

Offline Setting	Disabled ▼
-----------------	------------

Physical Storage

Storage	share01 🔍 ↻
Description	
Physical Storage Type	Remote

Submit **Delete** **Close**



Protection type is specified as 'Privacy' and secure the backend EMC VNX storage using AES 256-bit encryption and encryption key 'key01' managed at Thales nShield Connect.

Modify Virtual Storage Handler

Virtual Storage Protection Access Control Permissions

Virtual Storage Protection

Protection Type Privacy ▼

Encryption Keys

	Key Name	Last Update Datetime
1 <input type="checkbox"/>	key01	2014-02-13 10:09:11 +0800


Add Remove

Cryptographic Cipher

Cipher Algorithm AES ▼

Bit Length 256 ▼

Submit Close



CIFS storage protocol relies mainly on user-password authentication for access control. In this test, the Bloombase StoreSafe secure storage resource 'share01' is provisioned for user 'user01' with Microsoft Active Directory integration for user-password authentication and single sign-on.

Modify Virtual Storage Access Control

Virtual Storage Protection Access Control Permissions

User Access Control

Default ☐ Read ☐ Write

User Repository Microsoft Active Directory (MSAD) ▼

	User	Access Control List	Last Update Datetime
1 <input type="checkbox"/>	user01 ▼	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	2014-02-13 10:09:11 +0800

Add Remove

▼ More Options

Submit Close



Conclusion

Hardware security module

- Thales nShield Connect

passed all Bloombase interopLab's interoperability tests with Bloombase StoreSafe

Bloombase Product	Operating System	Hardware Security Module
Bloombase StoreSafe	Microsoft Windows Server	<ul style="list-style-type: none">• Thales nShield Connect
	Red Hat Enterprise Linux (RHEL)	<ul style="list-style-type: none">• Thales nShield Connect
	SUSE Linux Enterprise Server (SLES)	<ul style="list-style-type: none">• Thales nShield Connect
	Oracle Solaris	<ul style="list-style-type: none">• Thales nShield Connect
	IBM AIX	<ul style="list-style-type: none">• Thales nShield Connect
	HP-UX	<ul style="list-style-type: none">• Thales nShield Connect



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.

Acknowledgement

Bloombase InteropLab would like to thank Thales for supporting this interoperability testing.

Technical Reference

1. Bloombase StoreSafe Technical Specifications, <http://www.bloombase.com/content/8936QA88>
2. Bloombase StoreSafe Hardware Compatibility Matrix, <http://www.bloombase.com/content/e8Gzz281>
3. Thales nShield Connect, <https://www.thales-esecurity.com/products-and-services/products-and-services/hardware-security-modules/general-purpose-hsms/nshield-connect>
4. OASIS PKCS#11, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pkcs11