



Interoperability of Bloombase StoreSafe and nCipher nShield[®] XC for Data-at-Rest Encryption

January 2019



Executive Summary

nCipher nShield Connect XC 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 nCipher nShield Connect XC 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 have been tested with nCipher nShield Connect XC and Bloombase StoreSafe to secure Microsoft Storage Server on Microsoft Windows Server 2019 as the storage backend.

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.

© 2019 Bloombase, Inc.

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

nCipher nShield is trademark of nCipher Security 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-nCipher-nShield-XC-Interoperability-USLET-EN-Ro.94

Table of Contents

Table of Contents	3
Purpose and Scope	5
Assumptions	6
Infrastructure	7
Setup	7
Hardware Security Module	9
Bloombase StoreSafe	9
Storage System	9
Client Hosts	9
Configuration Overview	10
nCipher nShield	10
nCipher nShield Network Configuration	10
nCipher nShield Remote File System Setup	11
nCipher nShield Client Enrollment	12
nCipher Security World Setup	15
Microsoft Storage Server on Microsoft Windows Server 2019	15
Bloombase StoreSafe	18
nCipher nShield and Bloombase KeyCastle Integration	19
Encryption Key Provisioning	20
Backend Physical Storage Configuration	23
Secure Storage Configuration	24
Conclusion	28
Disclaimer	30
Acknowledgement	31
Technical Reference	32

Purpose and Scope

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

- Install and configure Bloomberg StoreSafe
- Integrate Bloomberg StoreSafe with nCipher nShield Connect XC
- Interoperability testing on client host systems including Linux, Windows, IBM AIX, HP-UX and Oracle Sun Solaris with Microsoft Storage Server as storage backend

Assumptions

This document describes interoperability testing of nCipher nShield with Bloombase StoreSafe. Therefore, it is assumed that you are familiar with operation of nCipher 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 nCipher 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 nCipher 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

Hardware Security Module

PKCS#11 Hardware Security Module | nCipher nShield Connect XC

Bloombase StoreSafe

Bloombase StoreSafe	Bloombase StoreSafe Software Appliance v3.4.7
nShield Client Security World Software Package	nCSS v12.50.4 Security World Software for Linux 64-bit
FIPS Mode	Non-strict FIPS security world
Server	VMware Virtual Machine (VM) on VMware ESXi 6.0
Processor	4 x Virtual CPU (vCPU)
Memory	8 GB

Storage System

Storage System | Microsoft Storage Server on Microsoft Windows Server 2019 on VMware ESXi 6.0

Client Hosts

Model	Dell PowerEdge R720	HPE ProLiant DL380 Gen8	IBM System x3650 M4	HPE Integrity rx2620	IBM System p5 510	Oracle Sun Fire x2100
Operating System	Microsoft Windows Server 2019	Red Hat Enterprise Linux 6	SUSE Linux Enterprise 11	HP-UX 11i	IBM AIX 7	Oracle Solaris 11

Configuration Overview

nCipher nShield

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

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

nCipher nShield Network Configuration

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

```
Network configuration
Enter IP address for
interface #1:
192.168.10.100
Enter netmask:
255.255.255.0
[ABORT] [NEXT]
```

nCipher nShield Remote File System Setup

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

nCipher 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/
```

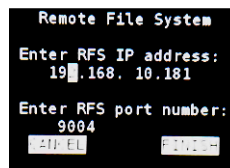
Configuration data (ESN and kneti hash) for RFS setup is acquired from nCipher nShield Connect.

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

Bloombase StoreSafe is provisioned as the Remote File System (RFS) for nCipher 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 nShield 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@storesafe ~]# enquiry
Server:
enquiry reply flags none
enquiry reply level Six
```

```

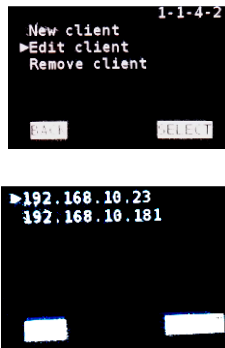
serial number      3C09-02E0-D947
mode               operational
version           12.50.4
speed index       15843
rec. queue        368..566
level one flags   Hardware HasTokens
version string    12.50.4-576-f8d14d5f46d3e97e711f1e370a75cc0ed7c4686e
nshield/nshield-project@6c1925ba, 3.4plal Built on Oct 10 2017 16:37:58,
Bootloader: 1.1.28, Security Processor: 2.1.18 , 12.40.2+ main
49f3fce0f950d27535ab8a49c0215f643fe66451 nshield/connect-project
checked in        000000005bb22c9f Mon Oct 1 07:18:07 2018
level two flags   none
max. write size   8192
level three flags KeyStorage
level four flags  OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd
ServerHasPollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable
HasFileOp HasLongJobs ServerHasLongJobs AESModuleKeys NTokenCmds
JobFragmentation LongJobsPreferred Type2Smartcard ServerHasCreateClient
HasInitialiseUnitEx Type3Smartcard HasKLF2
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      3C09-02E0-D947
mode               operational
version           3.4.1
speed index       15843
rec. queue        43..150
level one flags   Hardware HasTokens
version string    3.4plal Built on Oct 10 2017 16:37:58, Bootloader:
1.1.28, Security Processor: 2.1.18 , 12.40.2+ main
49f3fce0f950d27535ab8a49c0215f643fe66451 nshield/connect-project
checked in        0000000059dd2fa6 Tue Oct 10 13:37:58 2017
level two flags   none
max. write size   8192
level three flags KeyStorage
level four flags  OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd
ServerHasPollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable
HasFileOp HasLongJobs ServerHasLongJobs AESModuleKeys NTokenCmds
JobFragmentation LongJobsPreferred Type2Smartcard ServerHasCreateClient
HasInitialiseUnitEx Type3Smartcard HasKLF2
module type code  12
product name      nC3025E/nC4035E/nC4335N
device name      Rt14
EnquirySix version 6
impath kx groups  DHPrime1024 DHPrime3072
feature ctrl flags LongTerm
features enabled  RemoteShare StandardKM EllipticCurve ECCMQV
AcceleratedECC HSMHighSpeed
version serial    36
connection status OK
connection info   esn = 3C09-02E0-D947; addr = INET/213.121.187.217/9004;
ku hash = 077fd6a92e27b10b453a9daf7343eb3161e0b360, mech = Any
image version     12.40.2+
max exported modules 100
rec. LongJobs queue 42
SEE machine type  PowerPCELF
supported KML types DSAP1024s160 DSAP3072s256
using impath kx grp DHPrime3072
hardware status   OK

```

nCipher nShield Client Enrollment

Once RFS configuration is done, the nCipher 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@storeSAFE ~]# anonknet1 213.121.187.217
3C09-02E0-D947 077fd6a92e27b10b453a9daf7343eb3161e0b360
[root@storeSAFE ~]# nethsmenroll -p 213.121.187.217
Remote module returned ESN: 3C09-02E0-D947
HKNETI: 077fd6a92e27b10b453a9daf7343eb3161e0b360
Is the above correct? (yes/no): yes
OK configuring hardserver's nethsm imports
```

nCipher 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
```

nCipher 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 nCipher provided 'preload' utility for loading keys on a particular slot. Please refer to nCipher 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@storeSAFE ~]# /opt/nfast/bin/ckcheckinst
PKCS#11 library interface version 2.01
```

```

                flags 0
                manufacturerID "nCipher Corp. Ltd           "
                libraryDescription "nCipher PKCS#11 12.50.4+  "
                implementation version 12.50
                Loadsharing and Failover enabled

Slot  Status          Label
====  =====
    0  Fixed token    "loadshared accelerator  "
    1  Soft token     "nshield                 "

No removable tokens present.
Please insert an operator card into at least one available slot and
enter 'R' retry.
If you have not created an operator card or there are no physical
slots,
enter a fixed token slot number,
or 'E' to exit this program and create a card set before
continuing.

Enter a fixed token slot number, 'R'etry or '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 Bloombase 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 Bloombase StoreSafe

```
pkcs11-nfast.properties
```

property file.

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

nCipher Security World Setup

nCipher Security World is then initialized and set up.

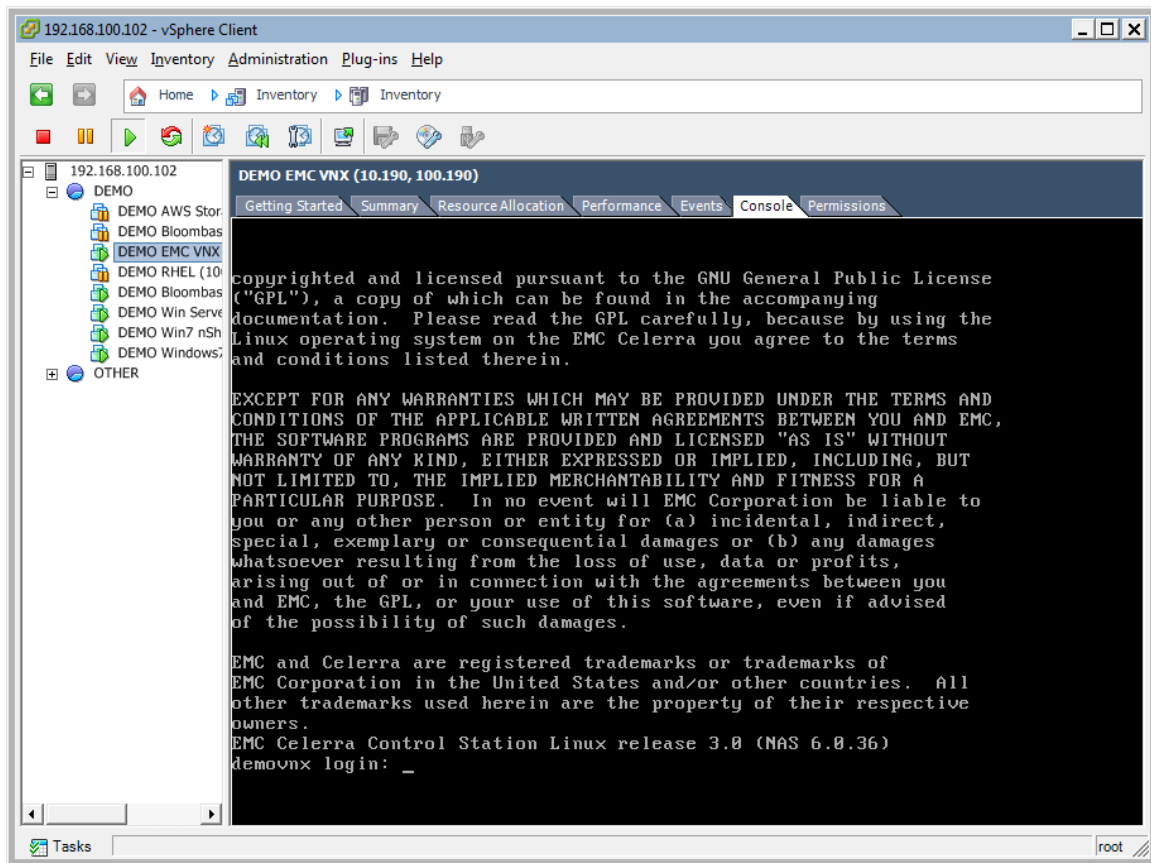


Please refer to “nShield Connect User Guide” for detailed setup and available configuration options.

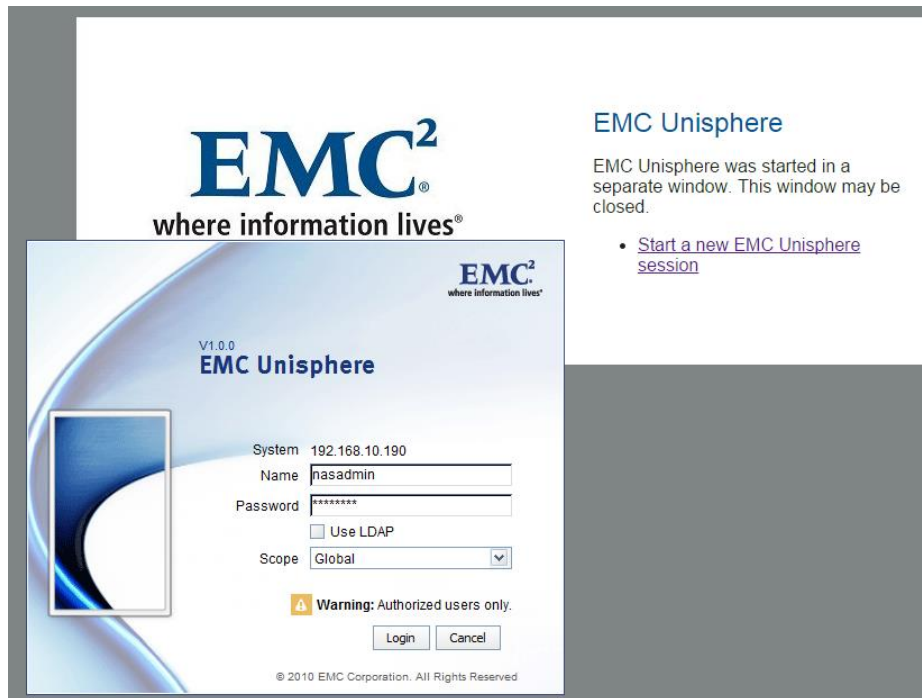
Note: the previous operations can be performed by any user in the nFast group; however, administrator access is needed for stopping and starting the hardserver.

Microsoft Storage Server on Microsoft Windows Server 2019

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



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

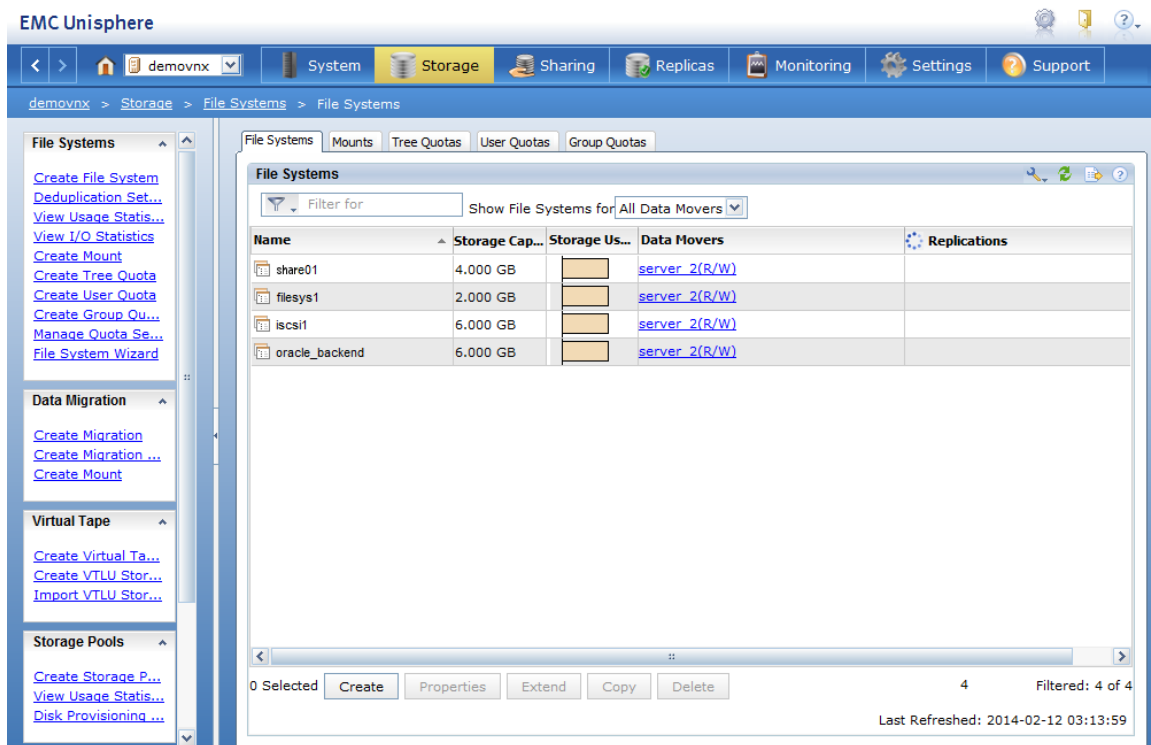


EMC Unisphere

EMC Unisphere was started in a separate window. This window may be closed.

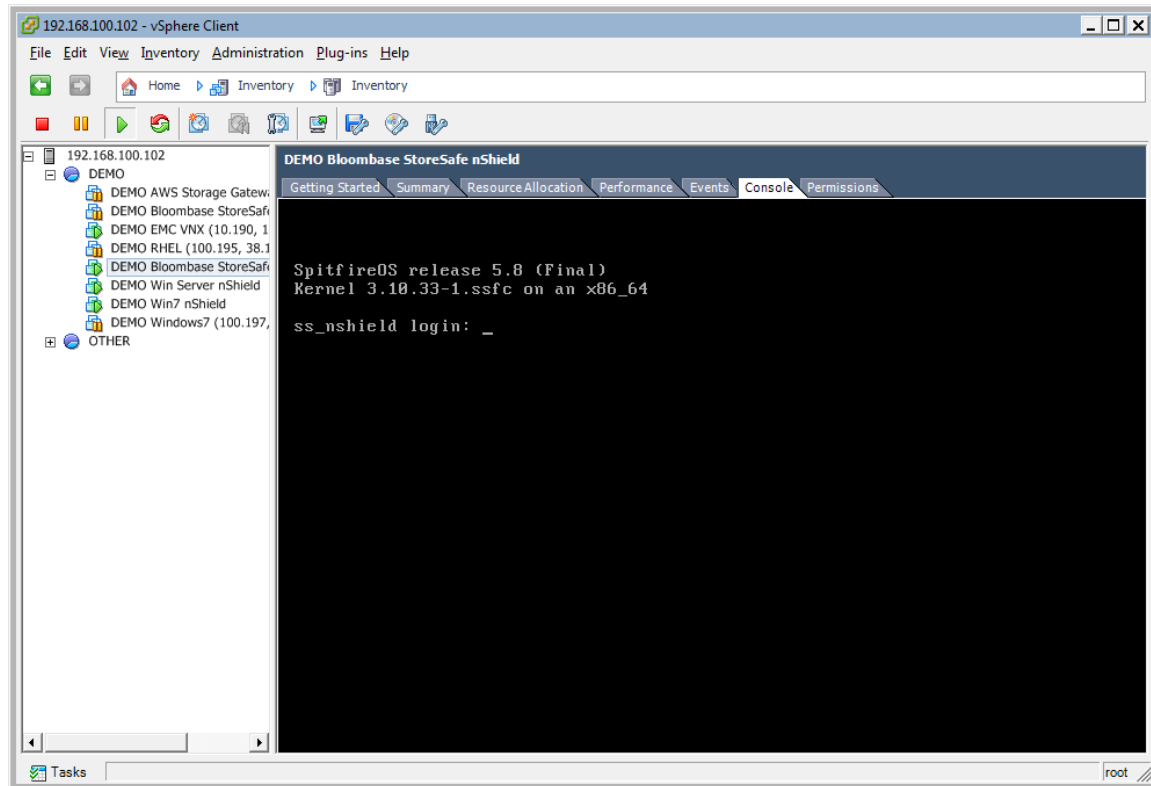
- [Start a new EMC Unisphere session](#)

iSCSI, SMB/CIFS and NFS storage services are provisioned on Microsoft Windows Storage Server to be used in this testing.

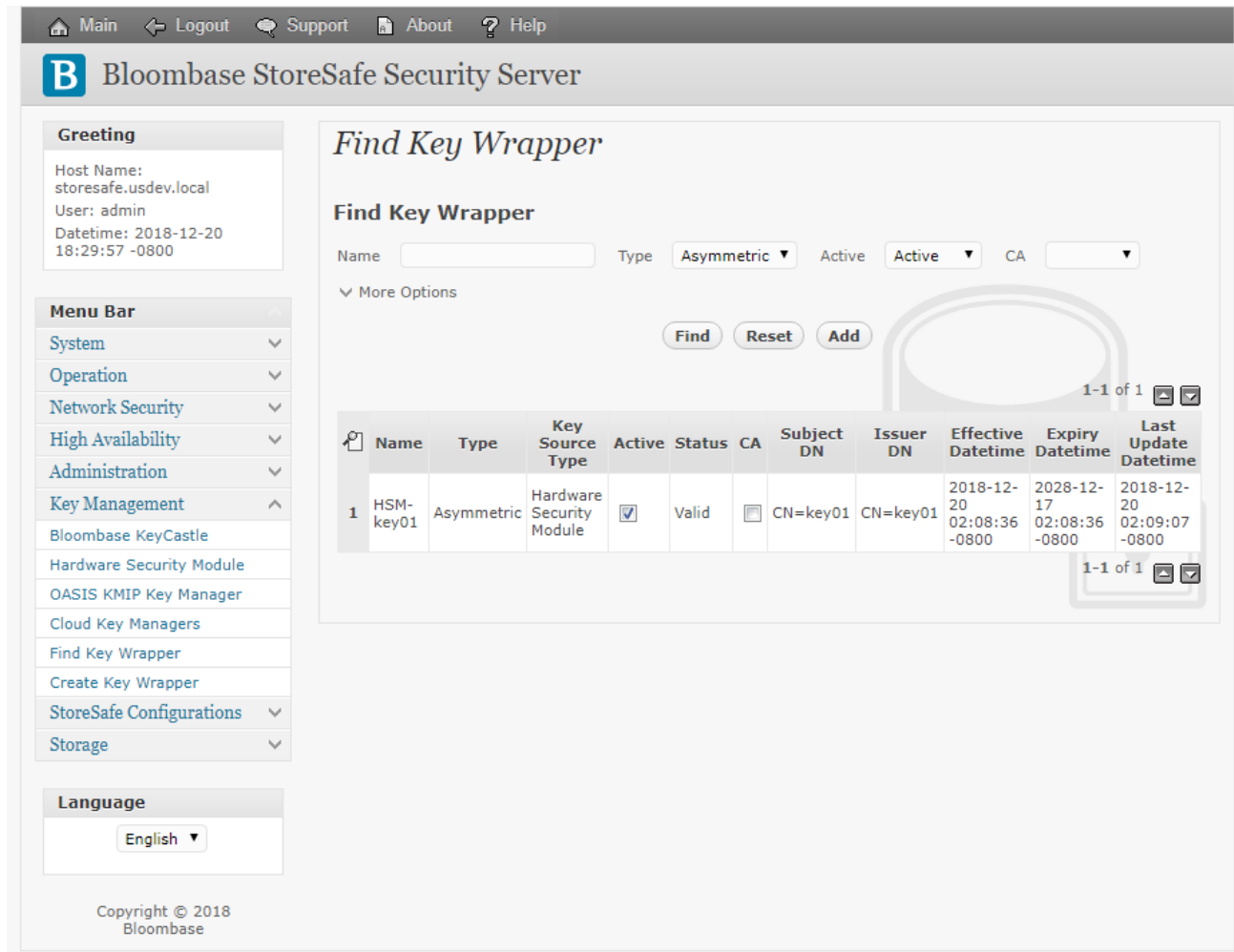


Bloombase StoreSafe

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 nCipher nShield Connect XC HSM.



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



nCipher nShield and Bloombase KeyCastle Integration

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

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

In this scenario, the nCipher nShield Connect XC 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 XC HSM and enter nShield OCS card pin.

Modify Hardware Security Module

Modify Hardware Security Module

Module: nfast

Label / Username: nshield

Pin: [Masked]

Confirm Pin: [Masked]

Buttons: Submit, Refresh, Delete, Cancel

When nCipher 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	15843	3C09-02E0-D947	12.40.2+ /	<input checked="" type="checkbox"/>

Buttons: Add


Encryption Key Provisioning

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

Modify Key Wrapper

Key Wrapper | **Permissions**

Modify Key Wrapper

Name	<input type="text" value="key01"/>
Key Source	Hardware Security Module
Type	Asymmetric
Active	<input checked="" type="checkbox"/>
Module	nfast
Label	nshield
Alias	<input type="text" value="key01"/>  HSM key alias missing
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 nCipher nShield Connect XC 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 XC 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

Module

Token

Key



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



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:

Description:

Active:

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



Protection type is specified as 'Privacy' and secure the Microsoft Storage Server storage backend using AES 256-bit encryption and encryption key 'key01' managed at nCipher nShield Connect XC.

Modify Virtual Storage Handler

Virtual Storage Protection Access Control Permissions

Virtual Storage Protection

Protection Type

Encryption Keys

	Key Name	Last Update Datetime
1	key01	2014-02-13 10:09:11 +0800

Cryptographic Cipher

Cipher Algorithm

Bit Length

SMB/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

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

More Options

Conclusion

Hardware security module

- nCipher nShield Connect XC

passed all Bloomberg interopLab's interoperability tests with Bloomberg StoreSafe

Bloomberg Product	Operating System	Hardware Security Module
Bloomberg StoreSafe	Microsoft Windows Server	• nCipher nShield Connect XC
	Red Hat Enterprise Linux (RHEL)	• nCipher nShield Connect XC
	SUSE Linux Enterprise Server (SLES)	• nCipher nShield Connect XC
	Oracle Solaris	• nCipher nShield Connect XC
	IBM AIX	• nCipher nShield Connect XC
	HP-UX	• nCipher nShield Connect XC

Disclaimer

The tests described in this paper were conducted in the Bloomberg InteropLab. Bloomberg has not tested this configuration with all the combinations of hardware and software options available. There may be significant differences in your configuration that will change the procedures necessary to accomplish the objectives outlined in this paper. If you find that any of these procedures do not work in your environment, please contact us immediately.

Acknowledgement

Bloombase InteropLab would like to thank nCipher 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. nCipher nShield General Purpose HSMs, <https://www.ncipher.com/products/general-purpose-hsms>
4. nCipher nShield Connect HSMs, <https://www.ncipher.com/products/general-purpose-hsms/nshield-connect>
5. OASIS PKCS#11, <https://www.oasis-open.org/committees/pkcs11/>
6. Bloombase as nCipher Security Partner, <https://www.ncipher.com/partners/bloombase>