Executive Summary

nCipher nShield Connect HSMs and nShield Remote Administration are validated by Bloombase InteropLab to run with Bloombase StoreSafe Intelligent Storage Firewall. This document describes the steps carried out to integrate nCipher nShield Connect HSMs and Remote Administration with Bloombase StoreSafe software appliance on VMware ESXi to deliver high resilient transparent storage encryption for mission critical applications. Client host system Microsoft Windows Server 2019 has been tested with nCipher nShield Connect HSMs, nShield Remote Administration and Bloombase StoreSafe to secure Microsoft Storage Server 2019 as storage backend.
Table of Contents
# Table of Contents

3

## Purpose and Scope

6

## Assumptions

7

## Infrastructure

8

### Setup

8

### Hardware Security Module

10

### Remote Administration

10

### Storage Encryption

10

### Storage System

10

### Application Client

11

## Configuration Overview

12

### nCipher nShield Connect HSMs

12

#### nCipher nShield Connect HSMs Network Configuration

12

#### nCipher nShield Connect Client Enrollment

12

#### nShield Failover Cluster Configuration

13

### nCipher nShield Remote Administration

14

#### nCipher nShield Remote Administration Client Configuration

14

#### nCipher Trusted Verification Device (TVD) Integration

15

#### nShield Remote Administration Cards Initialization and Operations

16

## Microsoft Storage Server on Microsoft Windows Server 2019

16

## Bloombase StoreSafe Intelligent Storage Firewall

18

#### nCipher nShield Connect HSM and Bloombase StoreSafe Integration

20

#### Encryption Key Provisioning

21

#### Backend Physical Storage Configuration

23

#### Secure Storage Configuration

23

#### Bloombase High Availability Module Configuration

26

## Use Case

28

### Data-at-Rest Encryption

28

### Bloombase StoreSafe High Availability Cluster Failover

30

### nCipher nShield Connect HSM Cluster Failover

31

### Bloombase StoreSafe High Availability Cluster Failback

33

### nCipher nShield Connect HSM Cluster Failback

34

## Conclusion

36

## Disclaimer

38

## Acknowledgement

39
Purpose and Scope

This document describes the steps necessary to integrate nCipher nShield Connect HSMs and Remote Administration with Bloombase StoreSafe to deliver agentless, transparent encryption security of traditional storage systems and next-generation storage services for mission-critical applications. Specifically, we cover the following topics:

- Install and configure Bloombase StoreSafe High-Availability (HA) cluster
- Integrate Bloombase StoreSafe with nCipher nShield Connect HSMs cluster and nShield Security World
- Integrate Bloombase StoreSafe with nCipher nShield Connect HSMs, nShield Remote Administration on Microsoft Windows 10
- Integrate application components Microsoft Windows Server 2019 client host system and Microsoft Storage Server 2019 with Bloombase StoreSafe and nCipher nShield to demonstrate how high resilient agentless data encryption could be achieved
Assumptions

This document describes the integration of nCipher nShield Connect HSMs and Remote Administration with Bloombase StoreSafe. It is assumed that you are familiar with operation of nCipher nShield Connect HSMs, nShield Remote Administration, 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 Connect HSMs and nShield Remote Administration are 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 Connect HSMs and nShield Remote Administration for your actual use cases. 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 https://www.bloombase.com or Bloombase SupPortal https://supportal.bloombase.com.
Infrastructure

Setup

The integration discussed in this guide is based on the system block diagram below:
## Hardware Security Module

<table>
<thead>
<tr>
<th>Hardware Security Module</th>
<th>nCipher nShield Connect XC HSMs v12.60.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Software</td>
<td>nCipher nCSS v12.60.11 Security World Software for Linux 64-bit</td>
</tr>
</tbody>
</table>

## Remote Administration

<table>
<thead>
<tr>
<th>Remove Administration</th>
<th>nCipher nCSS v12.60.11 Security World Software for Linux 64-bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Microsoft Windows 10</td>
</tr>
</tbody>
</table>

## Storage Encryption

<table>
<thead>
<tr>
<th>Bloombase StoreSafe</th>
<th>Bloombase StoreSafe Intelligent Storage Firewall Software Appliance v3.4.7.13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>VMware Virtual Machine (VM) on VMware ESXi 6.0</td>
</tr>
<tr>
<td>Processor</td>
<td>4 x Virtual CPU (vCPU)</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
</tr>
</tbody>
</table>

## Storage System

<table>
<thead>
<tr>
<th>Storage System</th>
<th>Microsoft Storage Server on Microsoft Windows Server 2019 on VMware ESXi 6.0</th>
</tr>
</thead>
</table>
# Application Client

<table>
<thead>
<tr>
<th>Client Host</th>
<th>Microsoft Windows Server 2019 on VMware ESXi 6.0</th>
</tr>
</thead>
</table>
Configuration Overview

nCipher nShield Connect HSMs

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 nCipher nShield Security World Software is complete, the HSM can be configured.

nCipher nShield Connect HSMs Network Configuration

The nCipher nShield Connect HSM is installed with network settings provisioned. In this integration as an example, the nCipher nShield Connect HSM is provided with IP address and Security World. The provided Security World files should be placed in the kmdata directory as stated in the nShield User Guide.

nCipher nShield Connect Client Enrollment

Bloombase StoreSafe software appliance then needs to be registered as the HSM client by nCSS enroll utility.
In this integration, Slot 1 has been used for key protection with the HSM as shown in the following entries in Bloombase StoreSafe

```
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

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

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

**nShield Failover Cluster Configuration**

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
```

Run command

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

as the sanity check to confirm if everything is working on the HSM and PKCS#11 layer. Ensure Loadsharing and Failover is enabled.

```
[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.

nCipher nShield Remote Administration

Please note that if using nShield Trusted Verification Device (TVD) 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 TVD 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.

nCipher nShield Remote Administration Client Configuration

To utilize a cardset with nShield Trusted Verification Device (TVD), the nCipher nShield Remote Administration Client must be installed on a physically accessible machine and the TVD attached to one of its ports.
If you are using and connected to multiple HSMs, you will see a list of them along with the associated ESNs. You will need to repeat this process for each ESN to ensure the cardset is active on them all and utilize high-availability.

**nCipher Trusted Verification Device (TVD) Integration**

When prompted, the user must insert a blank card into the Trusted Verification Device (TVD) slot. As with the below screen, the user must be present in-person to see the HSM ESN matches and confirm by pressing OK.
nShield Remote Administration Cards Initialization and Operations

Use the following command on a blank card inserted into the Trusted Verification Device (TVD) to create the operator cardset.

```
createocs -m 1 -p -Q 1/1 -N storesafe --remotely-readable
```

Repeat this step for every card in set inserting each one at a time into the Trusted Verification Device (TVD).

**Microsoft Storage Server on Microsoft Windows Server 2019**

Microsoft Storage Server on Microsoft Windows Server 2019 running on VMware ESXi is used in this interoperability test which is able to provide storage services over network storage protocols including NVMe, FCP, iSCSI, NFS, SMB, CIFS, REST, etc.
Microsoft Windows Server 2019 is deployed as a virtual appliance (VA) on VMware ESXi.
Microsoft Windows Server 2019 File Management is configured to provide the SMB share backend storage to domain users.

SMB/CIFS storage services are provisioned on Microsoft Windows Storage Server to be used in this integration testing.

**Bloombase StoreSafe Intelligent Storage Firewall**

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 HSMs.
Bloombase StoreSafe Intelligent Storage Firewall software appliance is deployed as a virtual appliance (VA) on VMware ESXi.
nCipher nShield Connect HSM and Bloombase StoreSafe Integration

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

Bloombase supports nCipher nShield Connect HSM out of the box. When a nCipher nShield Connect HSM is configured at Bloombase web management console, select Module as

\[ nfast \]

which allows the 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 HSM is assigned a token label namely

\[ storesafe \]
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.

When nCipher nShield Connect HSM resource is properly provisioned at Bloombase StoreSafe, the status would show up as

```
Active
```

**Encryption Key Provisioning**

To generate key in attached nCipher nShield Connect HSM, select Key Source Type as

```
Hardware Security Module
```

Module as

```
nfast
```
and the assigned HSM token label, in this case *storesafe*.

Select “Add Key” to generate a new key on the HSM.

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

Ensure you import a key from the HSM before you submit the key wrapper.
Backend Physical Storage Configuration

Physical storage namely

share01

is configured to be secured by Bloombase StoreSafe using encryption.

Secure Storage Configuration

Virtual storage namely

share01

of type

File
is created to virtualize physical storage

for application transparent encryption protection over network file protocols including CIFS and NFS.

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 HSM.
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.
Bloombase High Availability Module Configuration

A heartbeat network is set up between nodes in a Bloombase StoreSafe cluster to provide High Availability services. For this integration guide, the Bloombase StoreSafe nodes share a virtual IP resource to provide transparent failover.

The cluster synchronizes encryption configurations with all nodes in the cluster such as encryption keys from the nCipher nShield Connect HSM and encrypted data sources.
**View Cluster Status**

Cluster Enabled: **✓**

Name: **ssc**

## Nodes

<table>
<thead>
<tr>
<th></th>
<th>Enabled</th>
<th>Assigned Node Name</th>
<th>Node Name</th>
<th>Cluster</th>
<th>Host</th>
<th>Node Status</th>
<th>Role</th>
<th>System Status</th>
<th>Last Health Check</th>
<th>Last Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td>storesafe1.usdev.local</td>
<td>storesafe1.usdev.local</td>
<td>ssc</td>
<td>192.168.23.38</td>
<td>![Green Icon]</td>
<td>![Green Icon]</td>
<td>![Green Icon]</td>
<td>2020-10-27 08:51:23</td>
<td>0700</td>
</tr>
</tbody>
</table>

[Refresh] [Replicate] [Cancel]
Use Case

Data-at-Rest Encryption

SMB shares are an example from the many protocols Bloombase StoreSafe supports for encryption. A share from a Windows Server 2019 system that is accessible by domain users is created to act as backend storage. Bloombase StoreSafe creates a virtual encrypted share on its own hostname path that is accessed from a client software system.
On the demo virtual encrypted SMB share, a sample plaintext file is created by the client and saved. The file is transparently encrypted by the Bloombase StoreSafe encryption engine and stored on the Windows Server 2019 backend share.
If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.

Bloombase StoreSafe High Availability Cluster Failover

In the case of a Bloombase StoreSafe cluster node failure, a secondary or tertiary node will take over data path and encryption duties automatically after a specified timeout period.

From the client application perspective, no changes have been made. Besides a short interruption in the SMB share during failover, the file share path and data integrity are maintained.
nCipher nShield Connect HSM Cluster Failover

In the event of an nShield failure or timeout, the nfast driver will report the unavailable HSM module. As long as the failover and loadbalancing feature is enabled and the same cardset is inserted, the secondary or tertiary HSM module will automatically occupy the same slot.
The data encryption process will not have any interruption due to key caching. A new key generation or change to key configuration may be delayed during the timeout period.
Bloombase StoreSafe High Availability Cluster Failback

Once the primary Bloombase StoreSafe node returns to online status, the cluster configuration will show all nodes online and current active node. The administrator can then manually failback the primary node to active state.

The failback operation of Bloombase StoreSafe High Availability Cluster is fully transparent to users and software applications relying on the data path secured by Bloombase StoreSafe.
nCipher nShield Connect HSM Cluster Failback

Once any failed nShield HSM module returns to online status, the nfast driver will report the module status again with any active slot statuses.

The failback operation of nCipher nShield Connect HSM cluster is fully transparent to Bloombase StoreSafe with zero operational impact to users and software applications running on the Bloombase StoreSafe-secured storage resources.
Conclusion

In this integration guide, we have shown how to set up Bloombase StoreSafe Intelligent Storage Firewall high availability (HA) cluster with nCipher nShield Connect hardware security module (HSM) load-balancing cluster for security-hardened key management along with nCipher Remote Administration to achieve high security remote management of nCipher nShield HSMs. The end result is a security-accredited high resilient application-transparent storage encryption solution that locks down sensitive crown-jewel data on disks and helps mitigate information exfiltration threats for mission-critical systems and data services.

As a summary,

- nCipher nShield Connect hardware security module (HSM)
- nCipher Remote Administration
- Trusted Verification Device (TVD), and
- nCipher Security World

have been integrated with Bloombase StoreSafe Intelligent Storage Firewall to deliver encryption security of Microsoft Storage Server on Microsoft Windows Server 2019 over SMB/CIFS network storage protocols for software applications running on Microsoft Windows Server 2019 and Windows 10.
<table>
<thead>
<tr>
<th>Bloombase Product</th>
<th>Application Components</th>
<th>Hardware Security Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bloombase StoreSafe</td>
<td>• Microsoft Storage Server</td>
<td>• nCipher nShield Connect HSM</td>
</tr>
<tr>
<td>Intelligent Storage Firewall</td>
<td>• Microsoft Windows Server 2019</td>
<td>• nCipher Remote Administration</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows 10</td>
<td>• Trusted Verification Device (TVD)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• nCipher Security World</td>
</tr>
</tbody>
</table>
Disclaimer

The integration procedures 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 difference 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 the integration with Bloombase.
Reference

2. Bloombase StoreSafe Hardware Compatibility Matrix, https://www.bloombase.com/content/e8Gzz281
3. nCipher nShield Connect HSMs, https://www.ncipher.com/products/general-purpose-hsms/nshield-connect
5. nCipher nShield family of general purpose HSMs, https://www.ncipher.com/products/general-purpose-hsms