



# **Bloombase StoreSafe, nCipher nShield Connect HSMs and nShield Remote Administration Integration Guide for Data-at-Rest Encryption**

**October 2020**



## **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.

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.

© 2020 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 Connect HSMS and nShield Remote Administration Integration Guide - USLET-EN-Ro.94

# Table of Contents

<b>Table of Contents</b>	<b>3</b>
<b>Purpose and Scope</b>	<b>6</b>
<b>Assumptions</b>	<b>7</b>
<b>Infrastructure</b>	<b>8</b>
<b>Setup</b>	<b>8</b>
<b>Hardware Security Module</b>	<b>10</b>
<b>Remote Administration</b>	<b>10</b>
<b>Storage Encryption</b>	<b>10</b>
<b>Storage System</b>	<b>10</b>
<b>Application Client</b>	<b>11</b>
<b>Configuration Overview</b>	<b>12</b>
<b>nCipher nShield Connect HSMs</b>	<b>12</b>
nCipher nShield Connect HSMs Network Configuration	12
nCipher nShield Connect Client Enrollment	12
nShield Failover Cluster Configuration	13
<b>nCipher nShield Remote Administration</b>	<b>14</b>
nCipher nShield Remote Administration Client Configuration	14
nCipher Trusted Verification Device (TVD) Integration	15
nShield Remote Administration Cards Initialization and Operations	16
<b>Microsoft Storage Server on Microsoft Windows Server 2019</b>	<b>16</b>
<b>Bloombase StoreSafe Intelligent Storage Firewall</b>	<b>18</b>
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
<b>Use Case</b>	<b>28</b>
<b>Data-at-Rest Encryption</b>	<b>28</b>
<b>Bloombase StoreSafe High Availability Cluster Failover</b>	<b>30</b>
<b>nCipher nShield Connect HSM Cluster Failover</b>	<b>31</b>
<b>Bloombase StoreSafe High Availability Cluster Failback</b>	<b>33</b>
<b>nCipher nShield Connect HSM Cluster Failback</b>	<b>34</b>
<b>Conclusion</b>	<b>36</b>
<b>Disclaimer</b>	<b>38</b>
<b>Acknowledgement</b>	<b>39</b>

**Reference**

**40**

# 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.

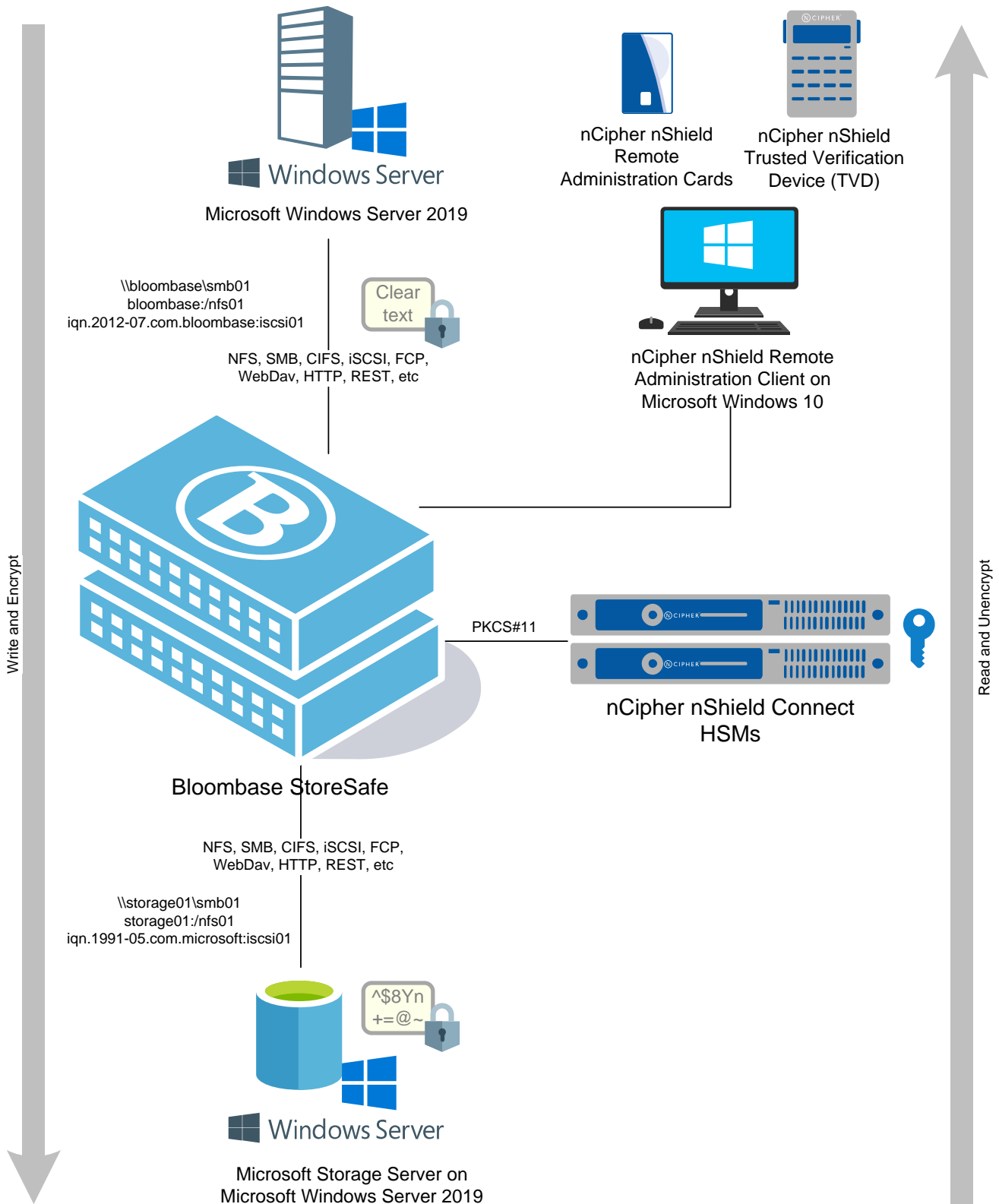
As nCipher nShield Connect HSMs and nShield Remote Administration are third party hardware option to Bloombase StoreSafe data at-rest encryption security solution, you are recommended to refer to installation and configuration guides of specific model of nCipher nShield Connect HSMs and nShield Remote 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

Hardware Security Module

Client Software

nCipher nShield Connect XC HSMs v12.60.2

nCipher nCSS v12.60.11 Security World Software for Linux 64-bit

## Remote Administration

Remote Administration

Client

nShield Remote Administration Client and Remote Administration Cards

Microsoft Windows 10

## Storage Encryption

Bloombase StoreSafe

Server

Processor

Memory

Bloombase StoreSafe Intelligent Storage Firewall Software Appliance v3.4.7.13

VMware Virtual Machine (VM) on VMware ESXi 6.0

4 x Virtual CPU (vCPU)

8 GB

## Storage System

Storage System

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

# Application Client

Client Host

Microsoft Windows Server 2019 on VMware ESXi 6.0

# 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 hardware. 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.



```

        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.

```

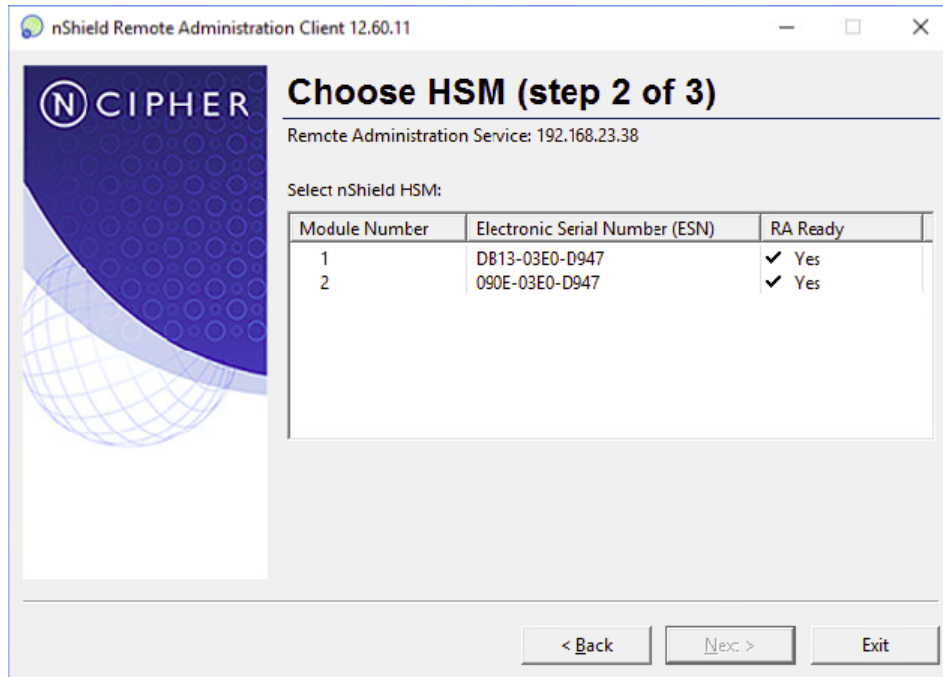
## nCipher nShield Remote Administration

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

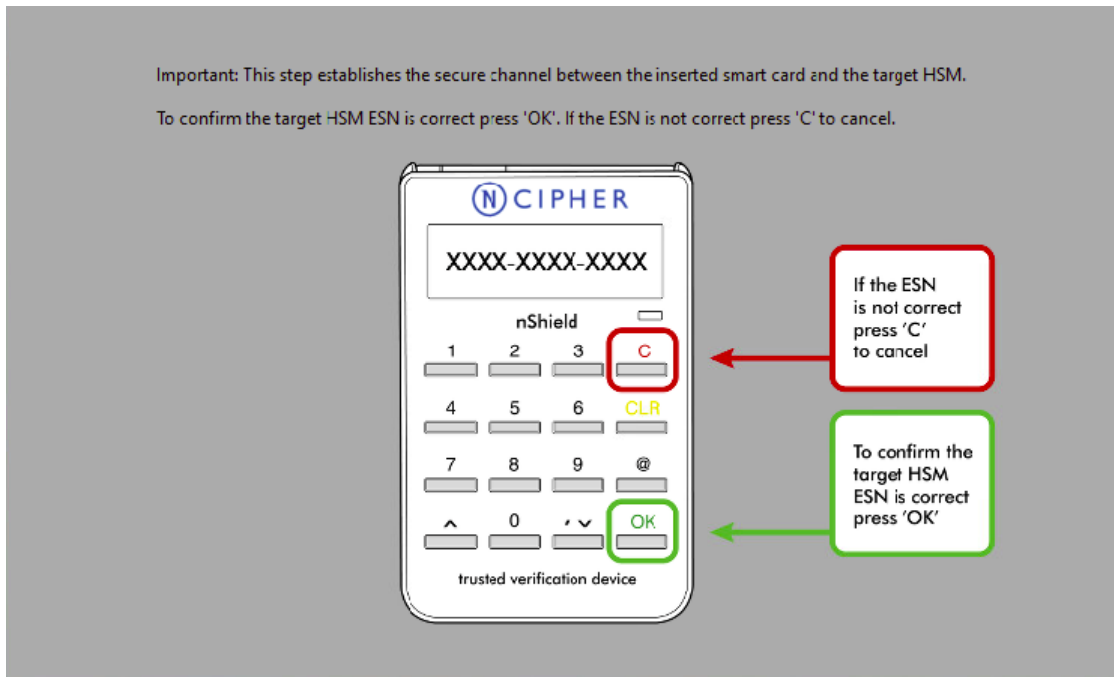
To utilize a cardset with nShield Trusted Verification Device (TVD), the nCipher nShield Remote Administration Client must be installed on a physically accessible machine and the TVD attached to one of its ports.

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.

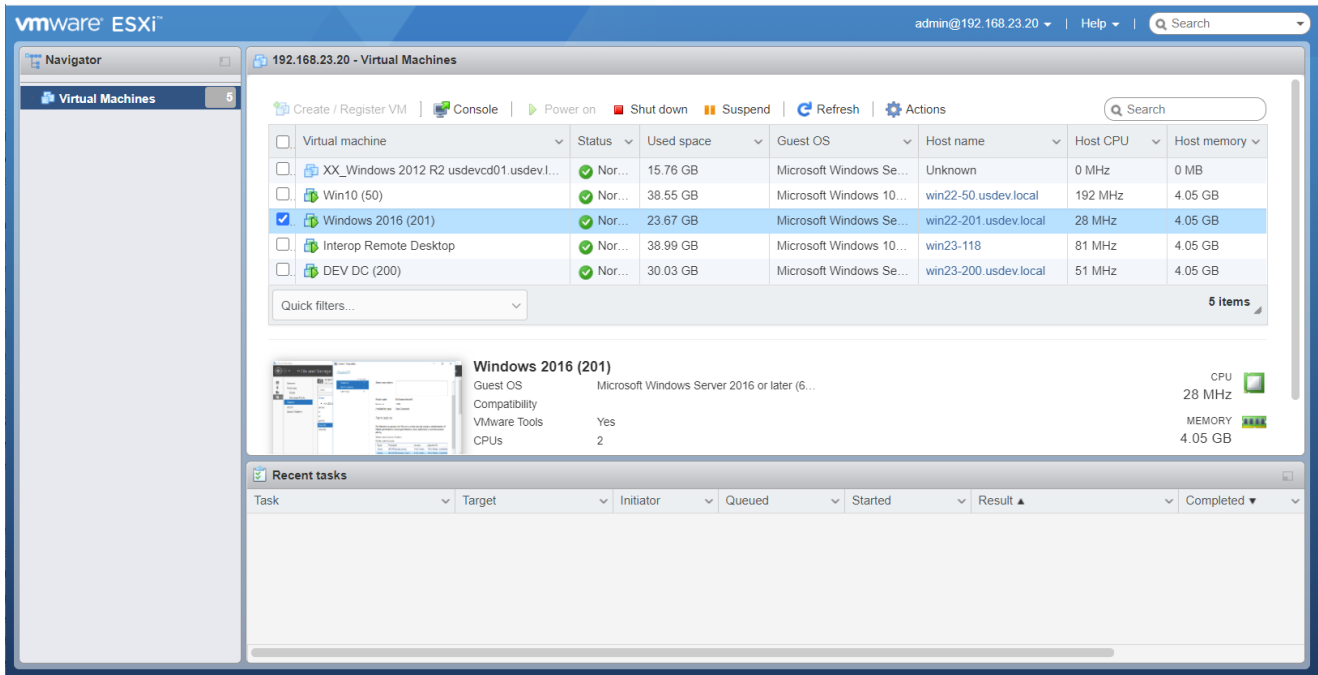
```
createocs -m 1 -p -Q 1/1 -N storesafe --remotely-readable
```

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

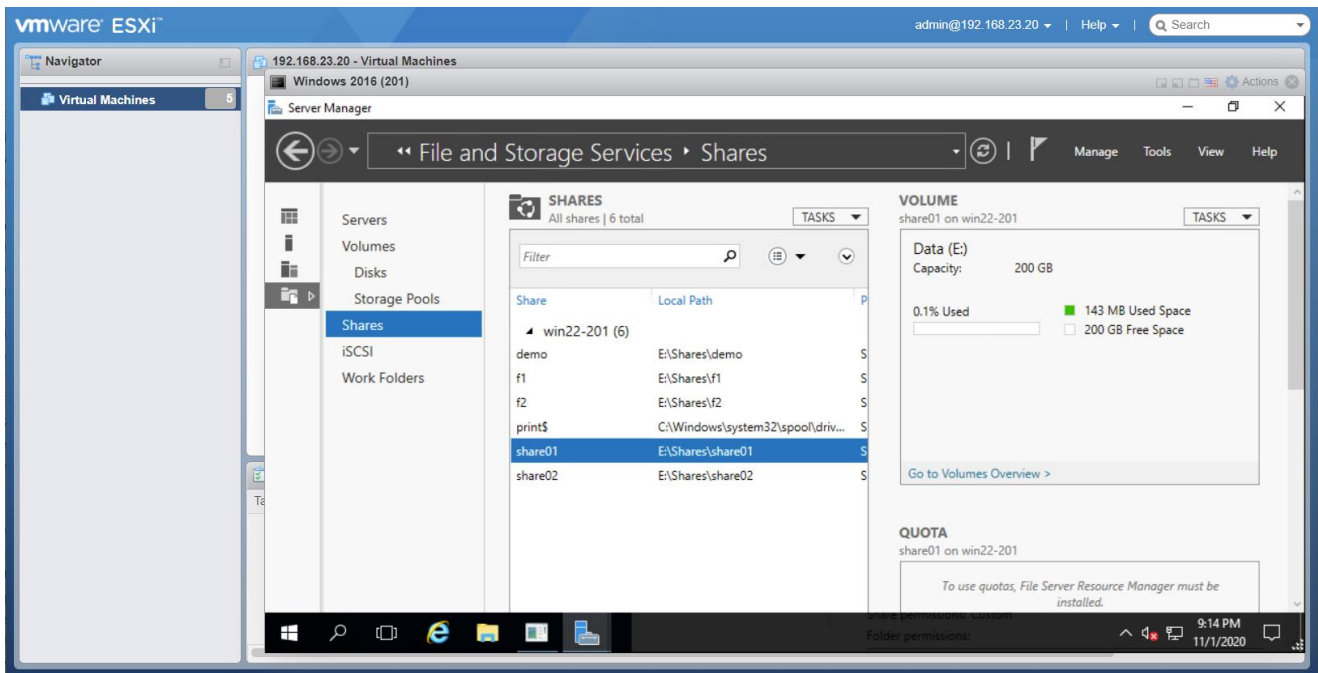
## Microsoft Storage Server on Microsoft Windows Server 2019

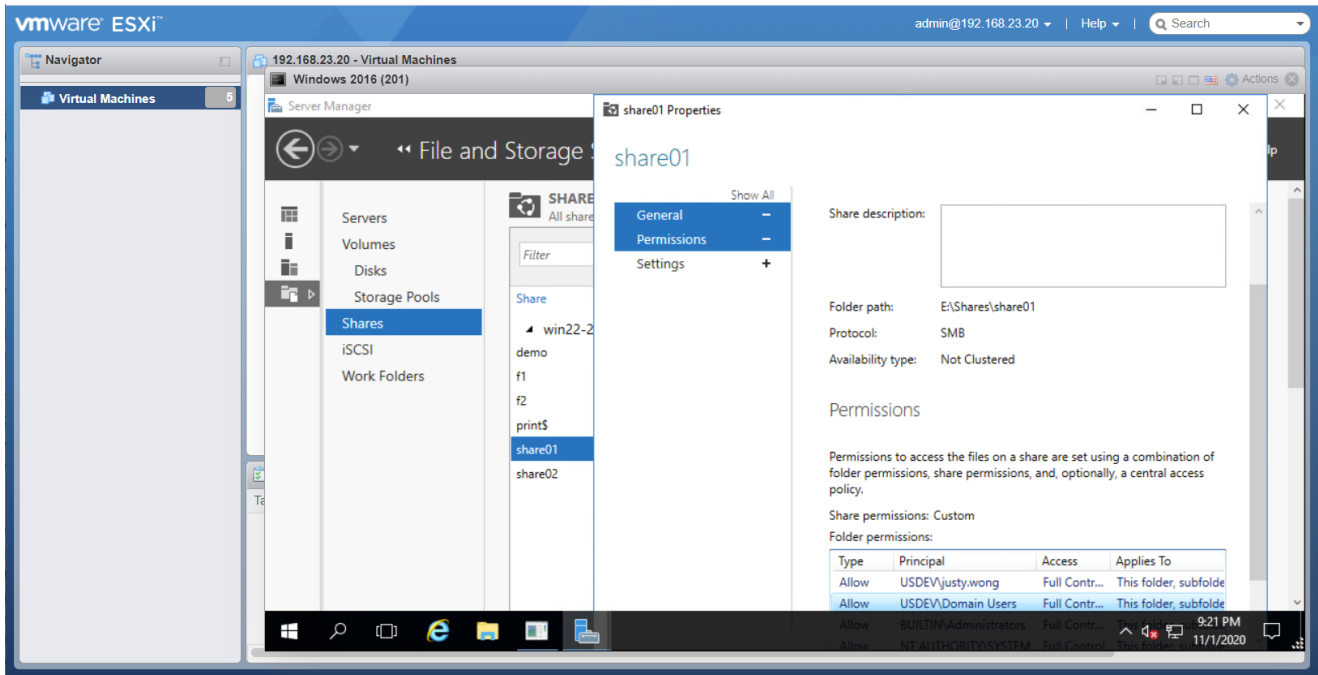
Microsoft Storage Server on Microsoft Windows Server 2019 running on VMware ESXi is used in this interoperability test which is able to provide storage services over network storage protocols including NVMe, FCP, iSCSI, NFS, SMB, CIFS, REST, etc.





Microsoft Windows Server 2019 is deployed as a virtual appliance (VA) on VMware ESXi.



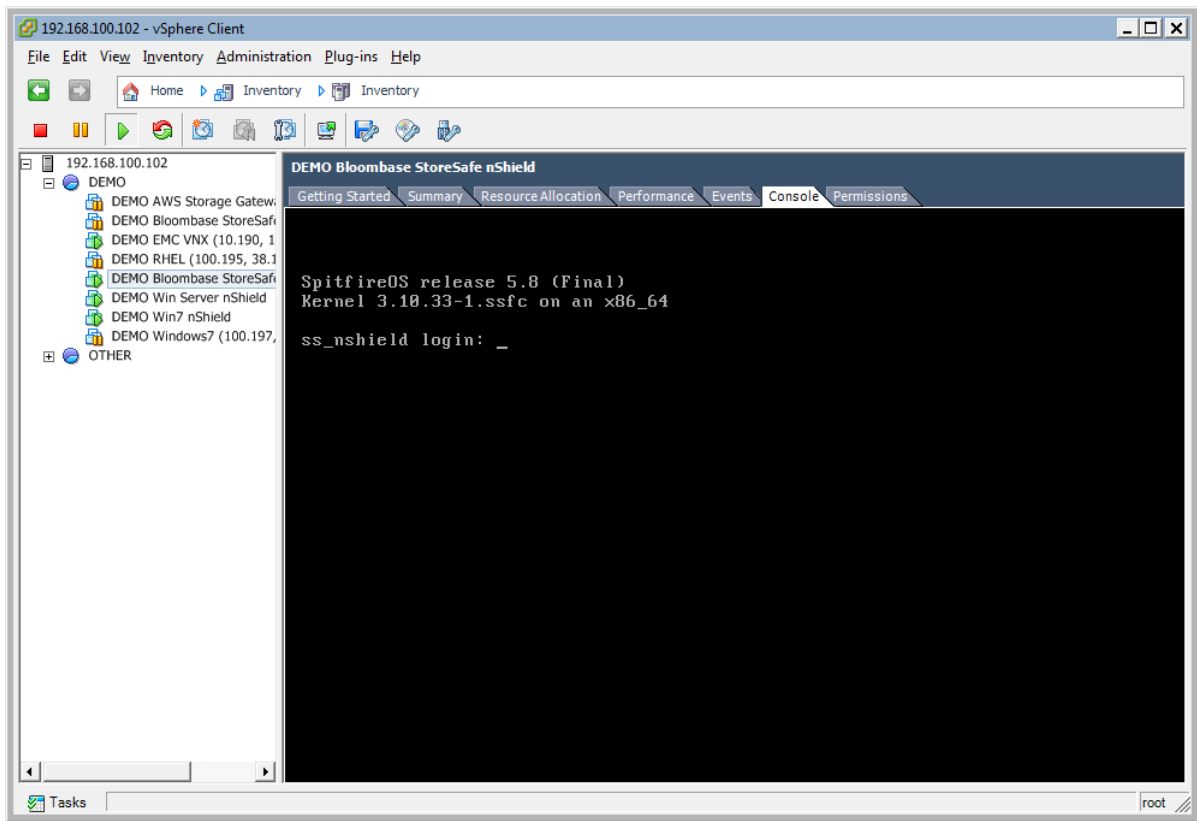


Microsoft Windows Server 2019 File Management is configured to provide the SMB share backend storage to domain users.

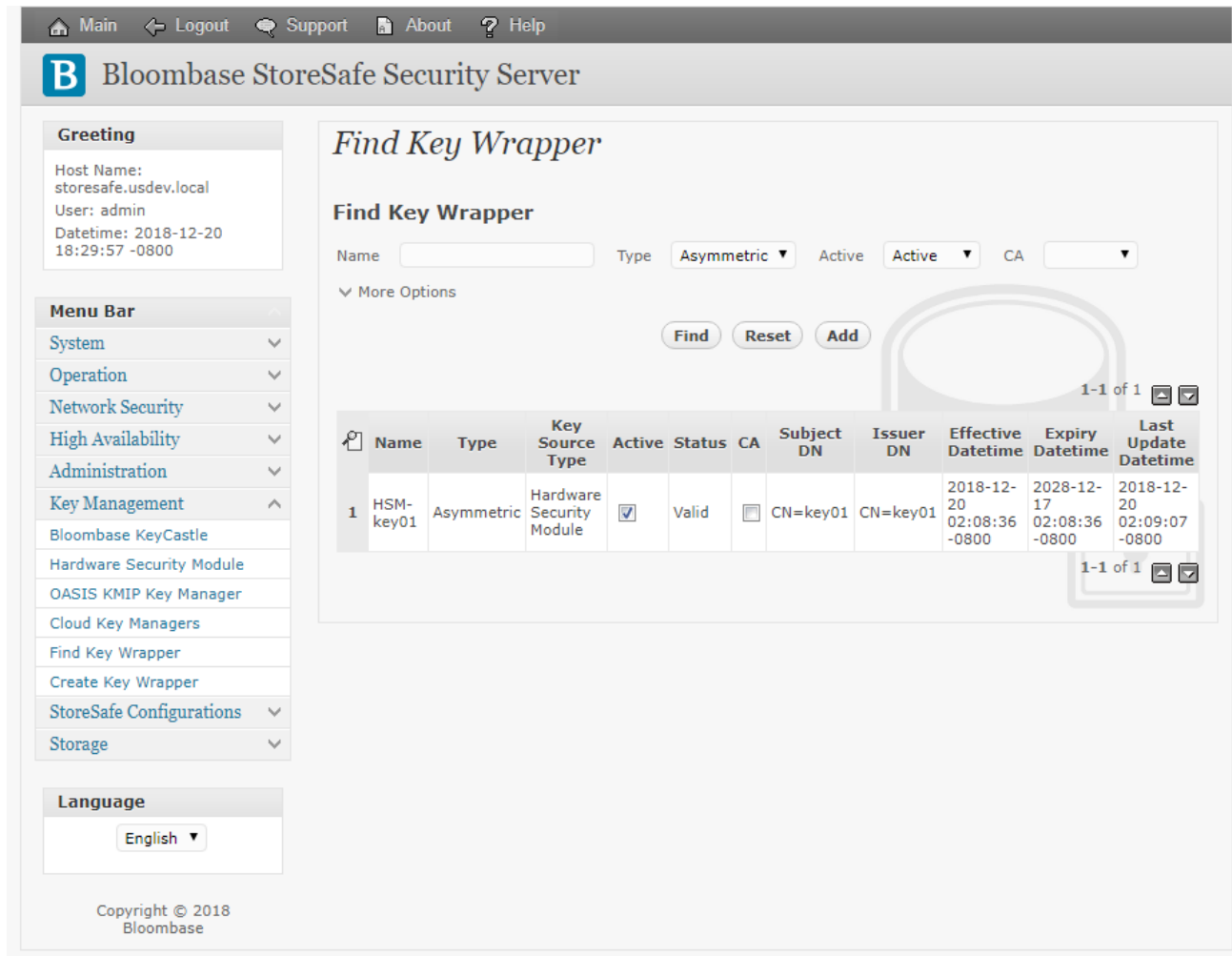
SMB/CIFS storage services are provisioned on Microsoft Windows Storage Server to be used in this integration testing.

## 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.

*Modify Hardware Security Module*

**Modify Hardware Security Module**

Module: nfast

Label / Username: storesafe

Pin: ●●●●●●

Confirm Pin: ●●●●●●

Buttons: Submit, Refresh, Delete, Cancel

When nCipher nShield Connect 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	storesafe	<input checked="" type="checkbox"/>		1	nfast	nCipher Corp. Ltd	nC3025E/nC4035E/nC4335N	DB13-03E0-D947 090E-03E0-D947	12.50.11 / 12.60.11	<input checked="" type="checkbox"/>

Buttons: Add

### Encryption Key Provisioning

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

Hardware Security Module

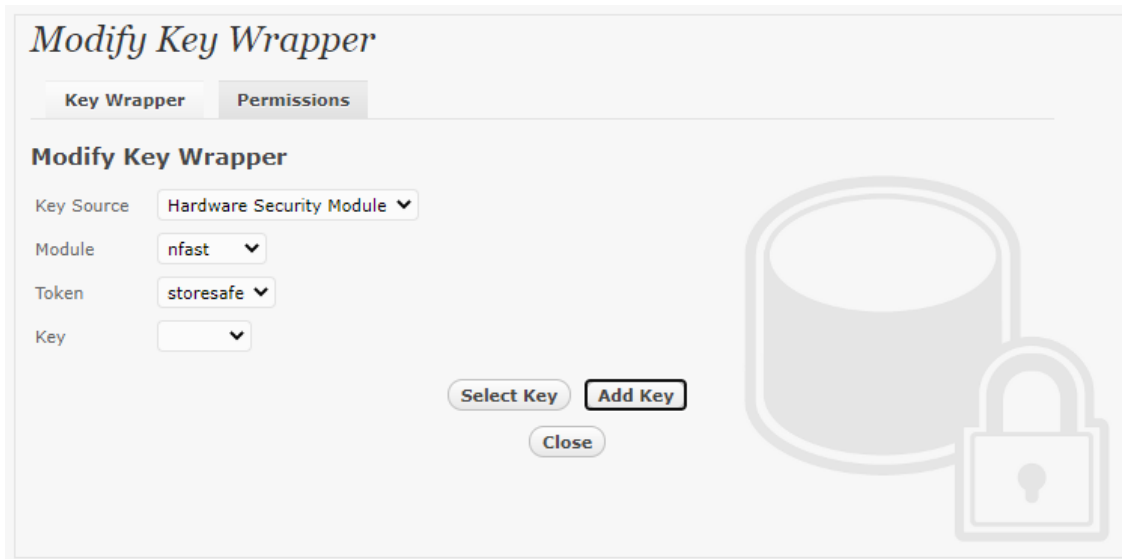
Module as

nfast

and the assigned HSM token label, in this case

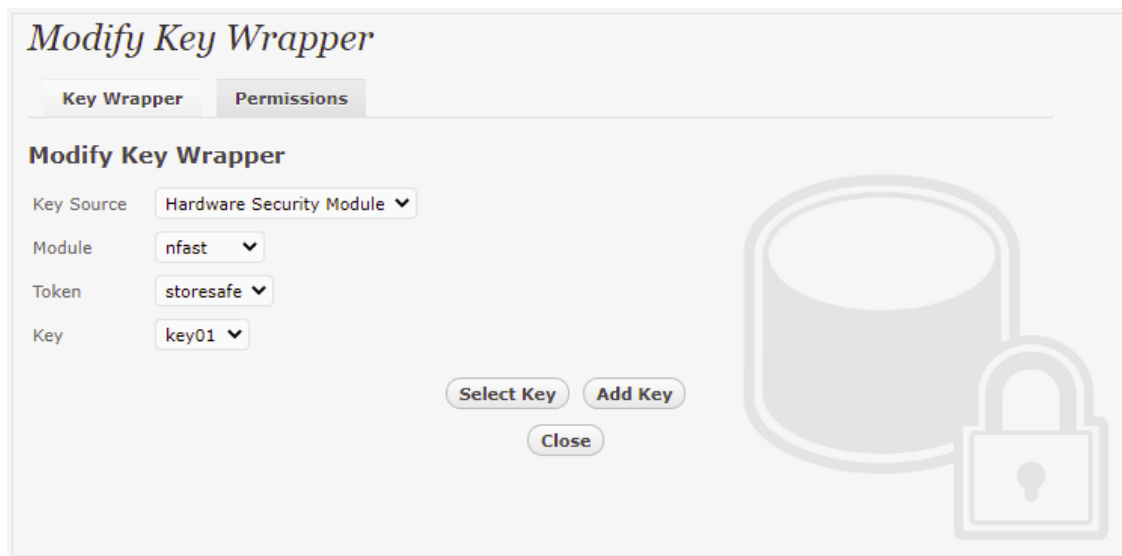
storesafe

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



The screenshot shows the 'Modify Key Wrapper' interface with the 'Key Wrapper' tab selected. The 'Key Source' is set to 'Hardware Security Module', 'Module' to 'nfast', and 'Token' to 'storesafe'. The 'Key' dropdown is empty. The 'Add Key' button is highlighted with a red border, while 'Select Key' and 'Close' are not. A large watermark of a key and a padlock is visible on the right side of the interface.

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



The screenshot shows the 'Modify Key Wrapper' interface with the 'Key Wrapper' tab selected. The 'Key Source' is set to 'Hardware Security Module', 'Module' to 'nfast', and 'Token' to 'storesafe'. The 'Key' dropdown now shows 'key01' selected. The 'Add Key' button is no longer highlighted. A large watermark of a key and a padlock is visible on the right side of the interface.

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.

*Modify Storage Configuration*

**Physical Storage**   **Permissions**

**Physical Storage Configuration**

Name: share01

Description: [Empty text area]

Physical Storage Type: Remote

Type: Common Internet File System (CIFS)

Host: 192.168.10.180

Share Name: share01

Read Size: [Empty text input]

Write Size: [Empty text input]

Synchronous:

Mount Hard:

User: Administrator

Password: [Empty text input]

Options: [Empty text input]

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

Status

Description

Active

Mode File

Owner admin

Last Update Datetime 2014-02-13 10:09:11 +0800

**Settings**

Offline Setting

**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 HSM.



### 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

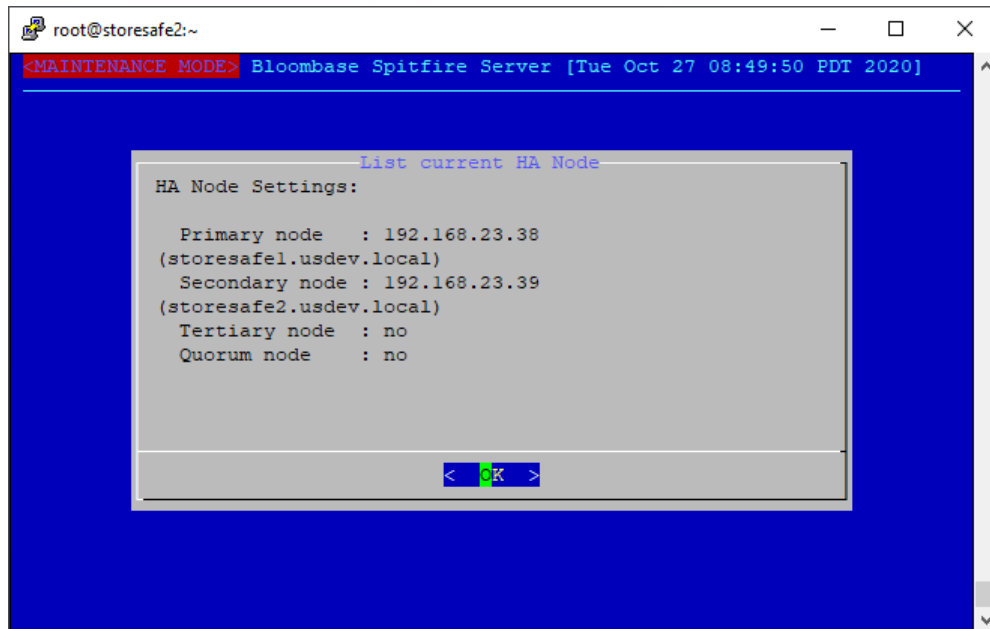
user01

with Microsoft Active Directory integration for user-password authentication and single sign-on.



## Bloombase High Availability Module Configuration

A heartbeat network is setup 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

### View Cluster Status

Cluster Enabled

Name

### Nodes

	Enabled	Assigned Node Name	Node Name	Cluster	Host	Node Status	Role	System Status	Last Health Check	Last Replication
1	<input checked="" type="checkbox"/>	storesafe1.usdev.local	storesafe1.usdev.local	ssc	192.168.23.38				 2020-10-27 08:51:23 -0700	
2	<input checked="" type="checkbox"/>	storesafe2.usdev.local	storesafe2.usdev.local	ssc	192.168.23.39				 2020-10-27 08:51:23 -0700	

Refresh

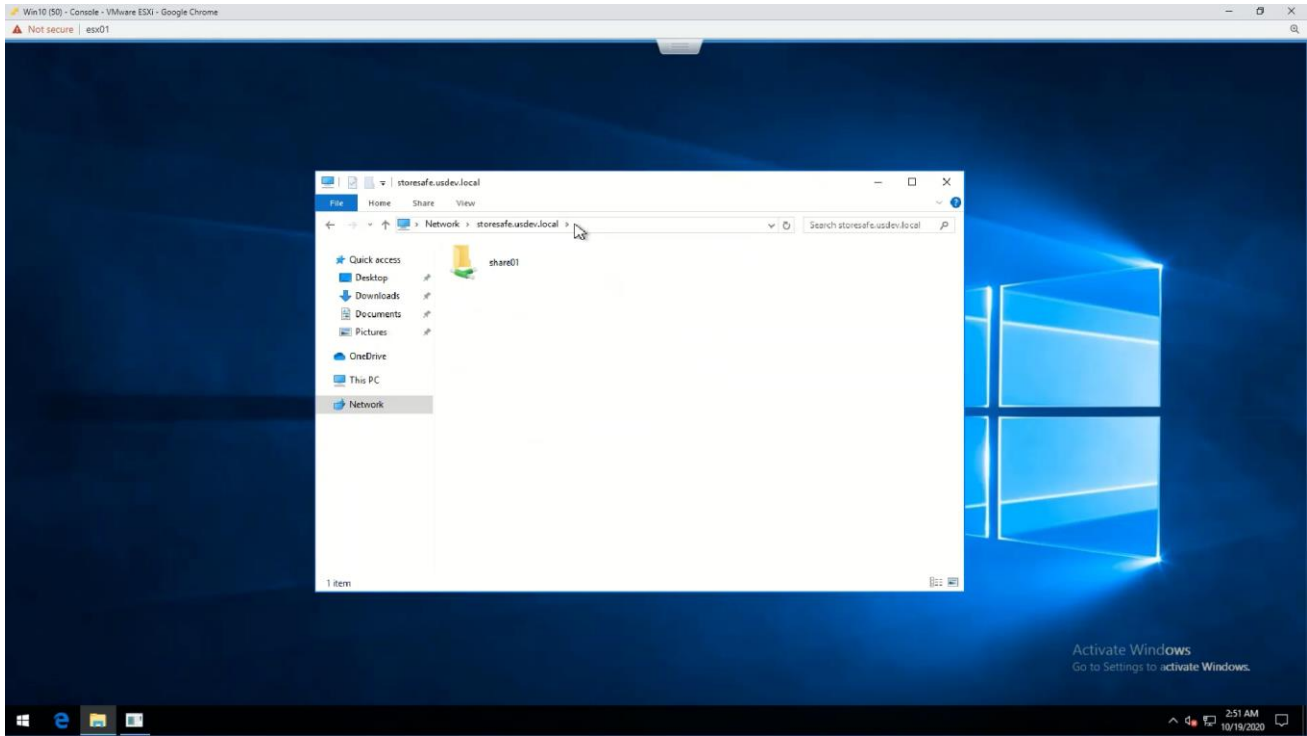
Replicate

Cancel

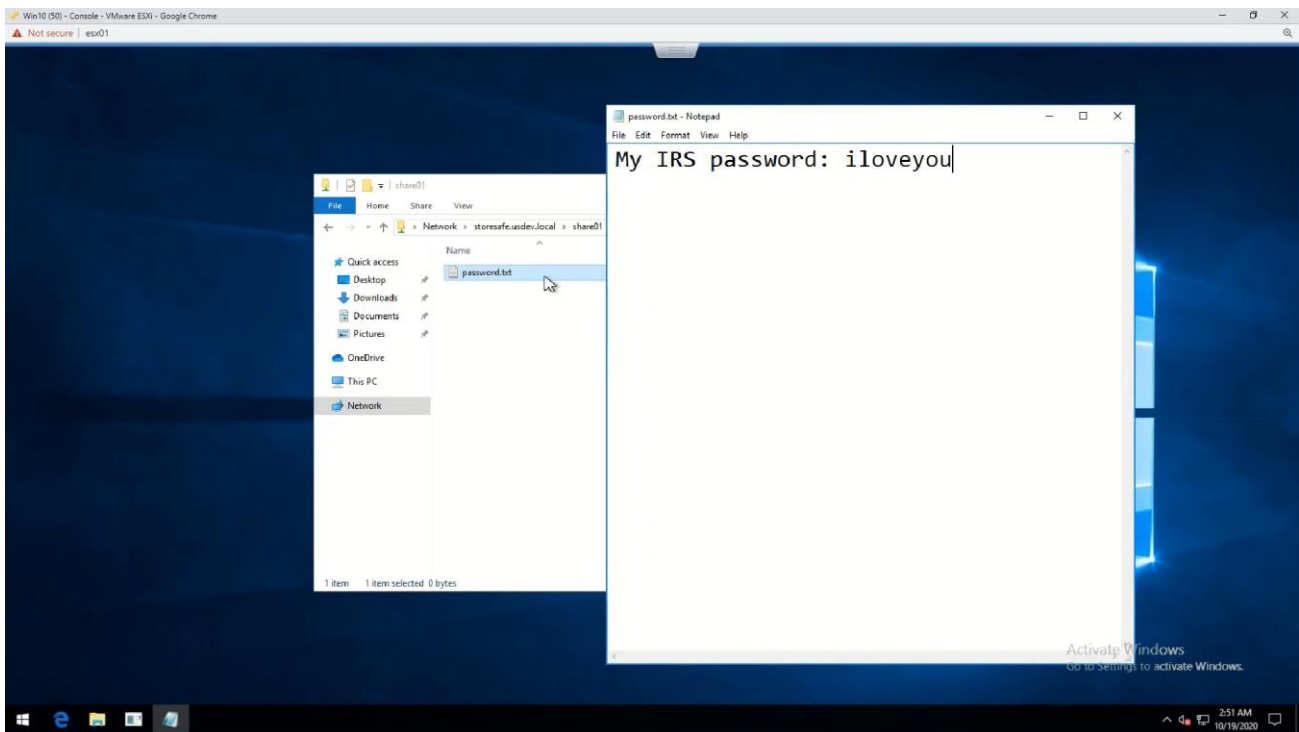
# Use Case

## Data-at-Rest Encryption

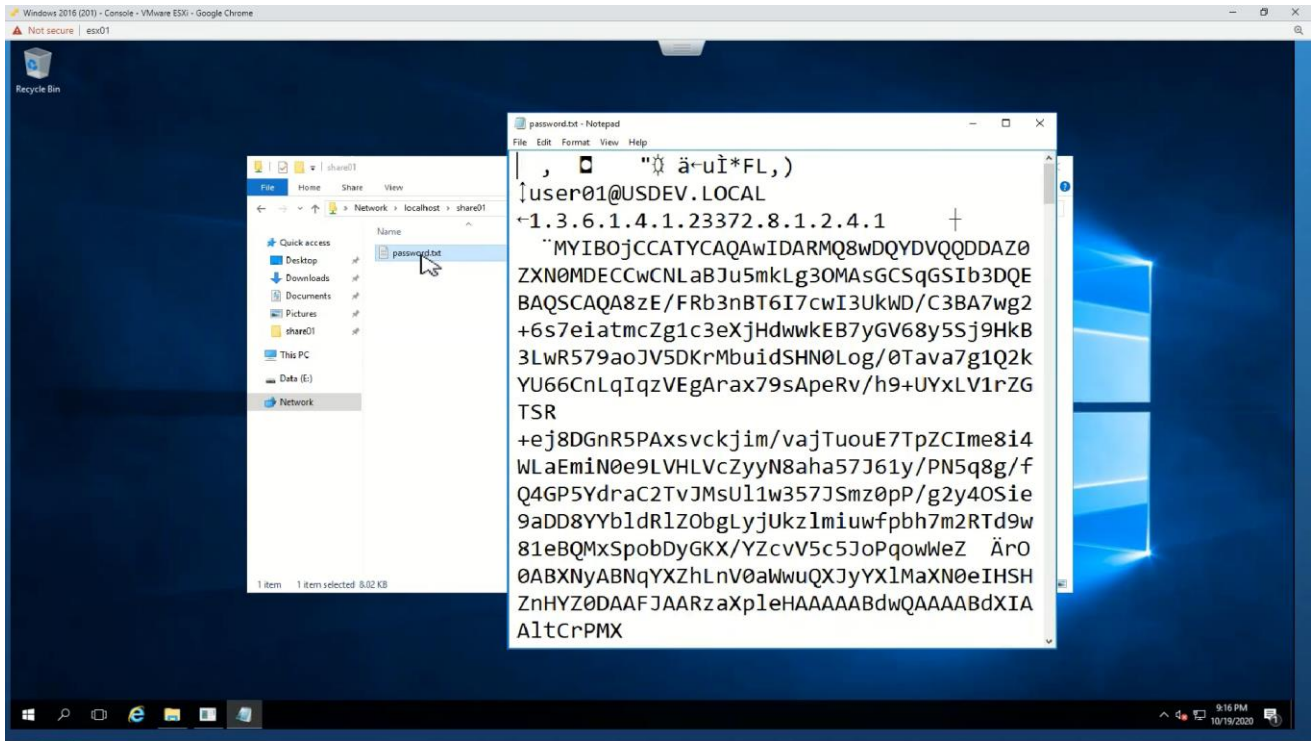
SMB shares are an example from the many protocols Bloomberg StoreSafe supports for encryption. A share from a Windows Server 2019 system that is accessible by domain users is created to act as backend storage. Bloomberg StoreSafe creates a virtual encrypted share on its own hostname path that is accessed 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.

*View Cluster Status*

**View Cluster Status**

Cluster Enabled

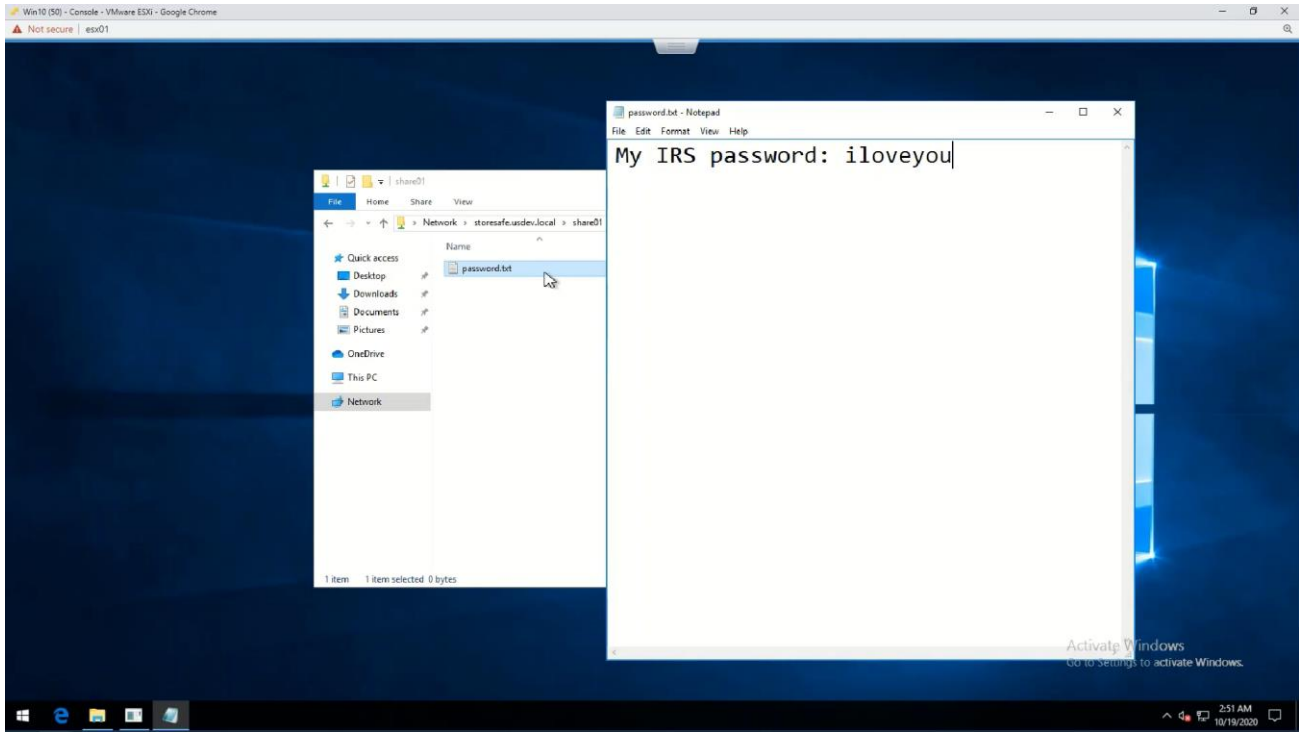
Name ssc

**Nodes**

Enabled	Assigned Node Name	Node Name	Cluster	Host	Node Status	Role	System Status	Last Health Check	Last Replication
<input checked="" type="checkbox"/>	storesafe1.usdev.local			192.168.23.38				2020-11-01 23:26:59 -0800	
<input checked="" type="checkbox"/>	storesafe2.usdev.local	storesafe2.usdev.local	ssc	192.168.23.39				2020-11-01 23:27:00 -0800	

Refresh Cancel

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.

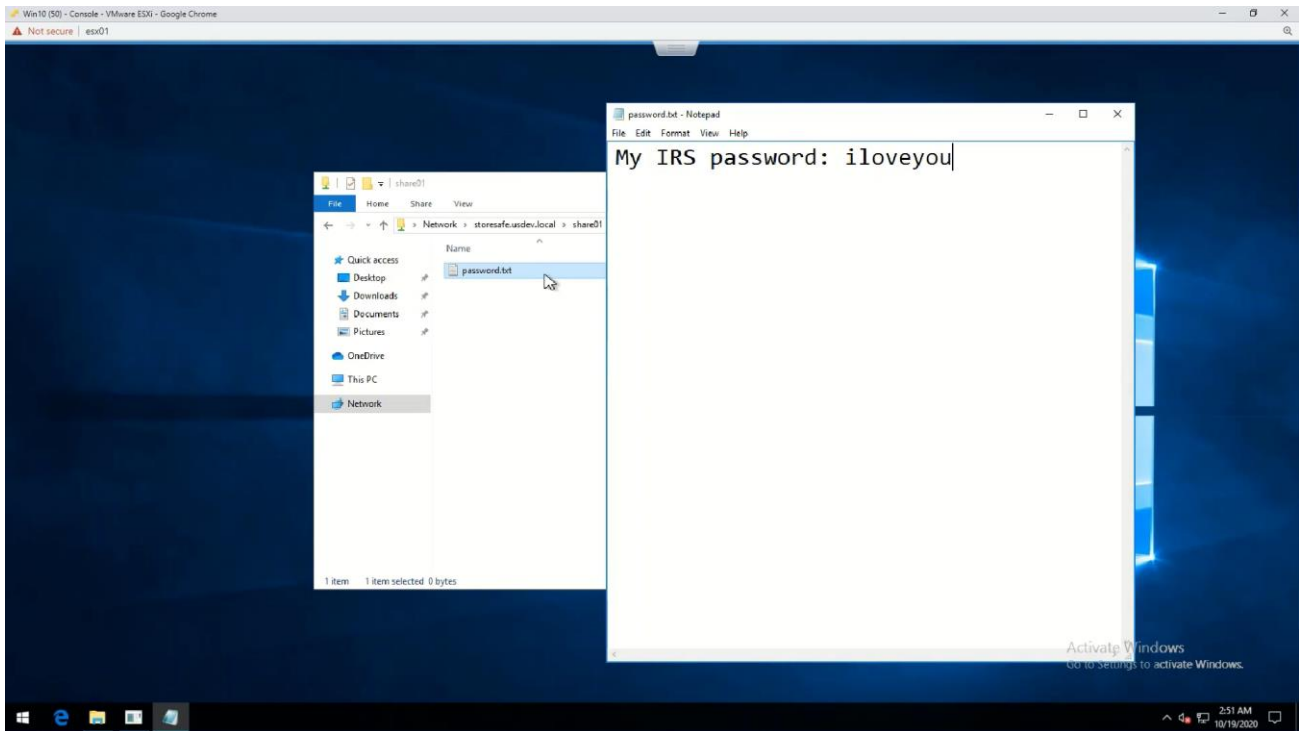
```
root@storeafe0:~#
hkfto          efc00bc51ad6c524726f2af9720d430a31b52c8c
hknull         0100000000000000000000000000000000000000000000000000
ex.client      none
k-out-of-n     1/8
other quora    m=1 r=1 nv=1 rtc=1 dsee=1 fto=1
createtime     2019-08-21 21:48:28
nso timeout    24 min
ciphersuite    DLF3072s256mAEScSP800131Ar1
min pp         0 chars
mode           none

Module #1
generation 1
state       0x8 Failed
flags       0x0 !ShareTarget
n_slots     0
esn         UNAVAILABLE
hkml        000000000000000000000000000000000000000000000000000
Module #1 - slot list unavailable

Module #2
generation 2
state       0x2 Usable
flags       0x10000 ShareTarget
n_slots     18
esn         090E-03E0-D947
hkml        ce39f897ead724b0909bff2c627d67b6c545a5a0

--More--
```

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.

## View Cluster Status

### View Cluster Status

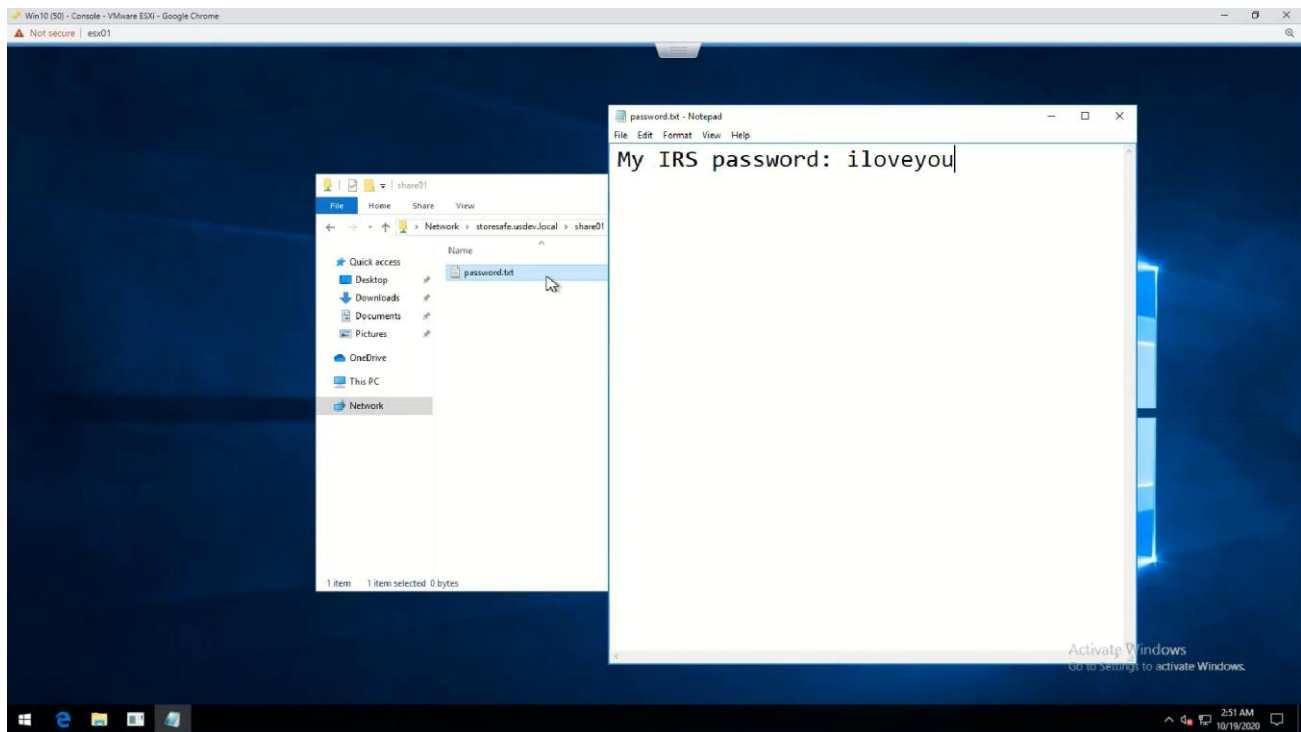
Cluster Enabled   
Name ssc

### Nodes

Enabled	Assigned Node Name	Node Name	Cluster	Host	Node Status	Role	System Status	Last Health Check	Last Replication
<input checked="" type="checkbox"/>	storesafe1.usdev.local	storesafe1.usdev.local	ssc	192.168.23.38				2020-11-02 00:09:14 -0800	
<input checked="" type="checkbox"/>	storesafe2.usdev.local	storesafe2.usdev.local	ssc	192.168.23.39				2020-11-02 00:09:18 -0800	

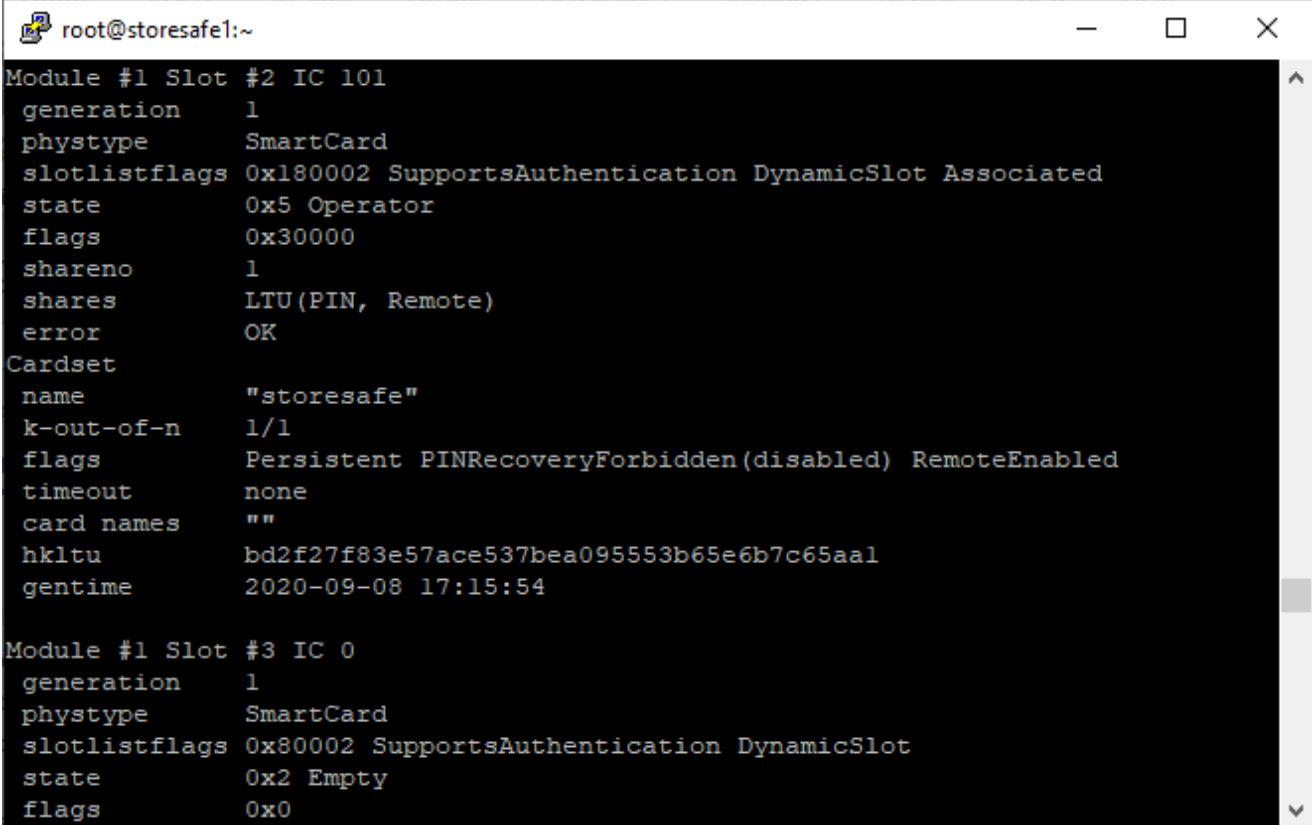
Refresh Cancel

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.



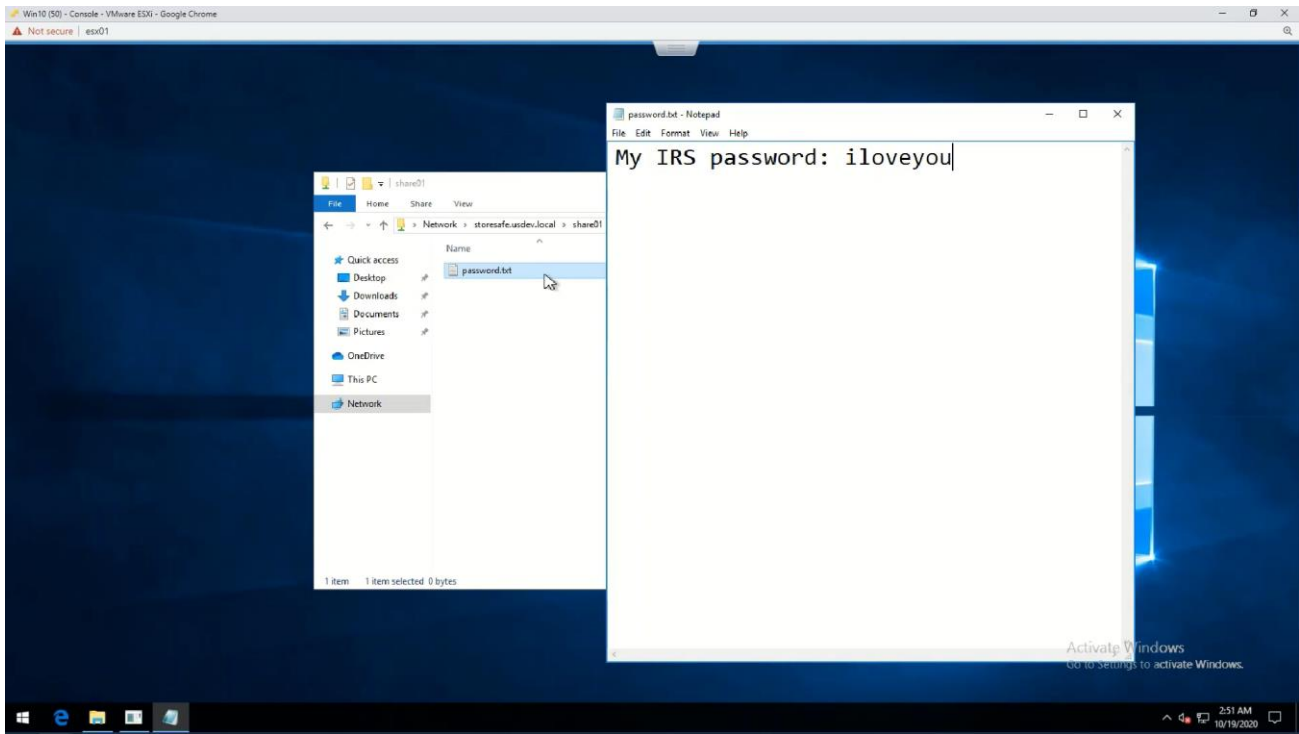
## nCipher nShield Connect HSM Cluster Failback

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



```
root@storesafe1:~  
Module #1 Slot #2 IC 101  
generation      1  
phystype        SmartCard  
slotlistflags   0x180002 SupportsAuthentication DynamicSlot Associated  
state           0x5 Operator  
flags           0x30000  
shareno         1  
shares          LTU(PIN, Remote)  
error           OK  
Cardset  
name            "storesafe"  
k-out-of-n      1/1  
flags           Persistent PINRecoveryForbidden(disabled) RemoteEnabled  
timeout         none  
card names      ""  
hkltu           bd2f27f83e57ace537bea095553b65e6b7c65aa1  
gentime         2020-09-08 17:15:54  
  
Module #1 Slot #3 IC 0  
generation      1  
phystype        SmartCard  
slotlistflags   0x80002 SupportsAuthentication DynamicSlot  
state           0x2 Empty  
flags           0x0
```

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.

Bloombase Product	Application Components	Hardware Security Module
Bloombase StoreSafe Intelligent Storage Firewall	<ul style="list-style-type: none"> <li>• Microsoft Storage Server</li> <li>• Microsoft Windows Server 2019</li> <li>• Microsoft Windows 10</li> </ul>	<ul style="list-style-type: none"> <li>• nCipher nShield Connect HSM</li> <li>• nCipher Remote Administration</li> <li>• Trusted Verification Device (TVD)</li> <li>• nCipher Security World</li> </ul>

# Disclaimer

The integration procedures 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 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

1. Bloombase StoreSafe Technical Specifications, <https://www.bloombase.com/content/8936QA88>
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>
4. nCipher nShield Remote Administration, <https://www.ncipher.com/products/hsm-management-and-monitoring/nshield-remote-administration>
5. nCipher nShield family of general purpose HSMs, <https://www.ncipher.com/products/general-purpose-hsms>
6. nCipher nShield-as-a-Service (nSaaS), <https://www.ncipher.com/products/general-purpose-hsms/nshield-as-a-service>
7. OASIS PKCS#11, [https://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=pkcs11](https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pkcs11)
8. Bloombase is nCipher Security Partner, <https://www.ncipher.com/partners/bloombase>