interopLab

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

October 2020

BLOOMBASE®

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.

Document No.: BLBS-TN - Bloombase StoreSafe nCipher nShield Connect HSMs and nShield Remote Administration Integration Guide - USLET-EN-R0.95

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

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

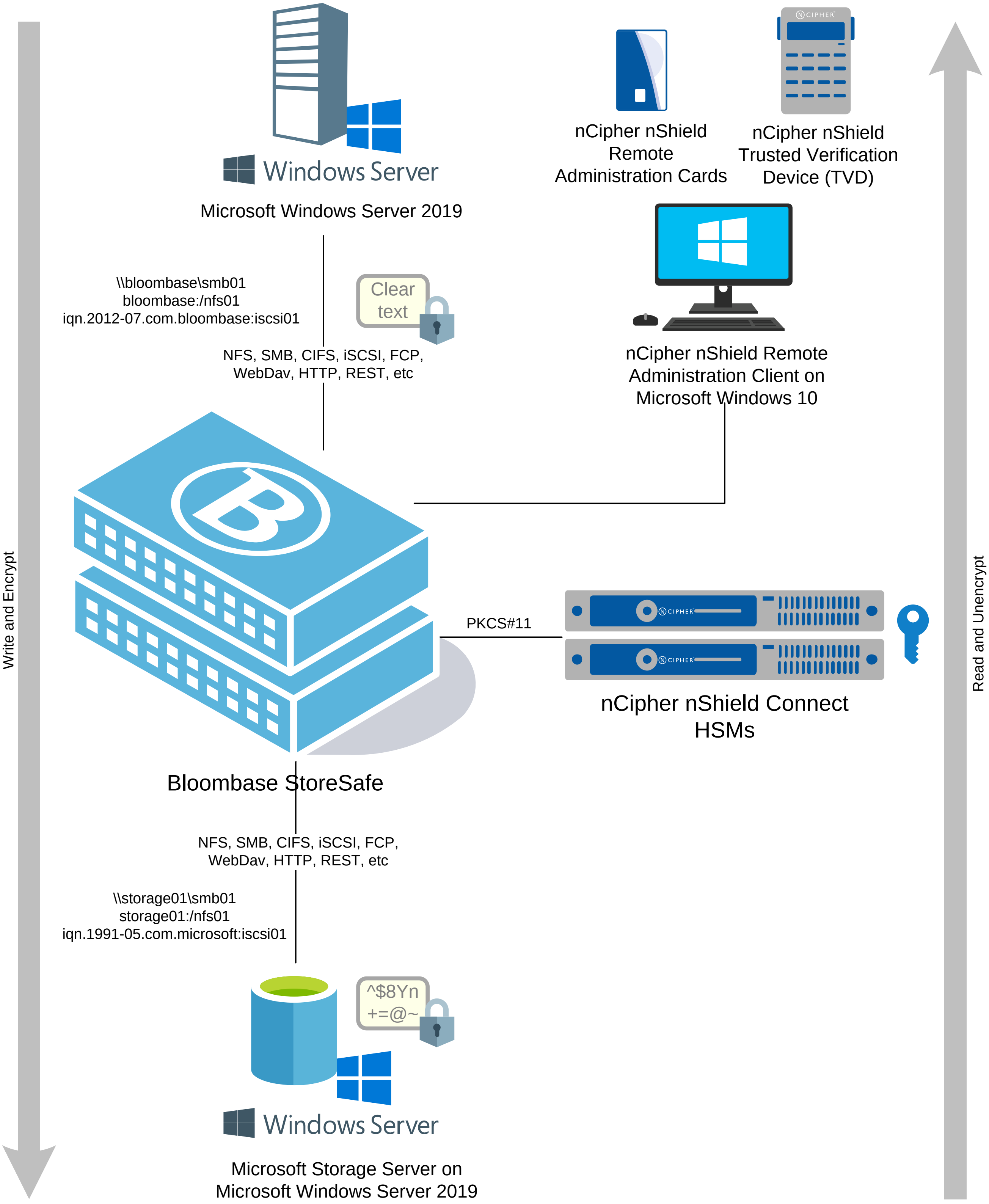
This document describes the integration of nCipher nShield Connect HSMs and Remote Administration with Bloombase StoreSafe. It is assumed that you are familiar with operation of nCipher nShield Connect HSMs, nShield Remote Administration, storage systems, and major operating systems including Linux, 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:


Windows Server
Microsoft Windows Server 2019
nCipher nShield Remote Administration Cards
nCipher nShield Trusted Verification Device (TVD)
\\bloombase\smb01
bloombase:/nfs01
iqn.2012-07.com.bloombase:iscsi01
Clear text
NFS, SMB, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
nCipher nShield Remote Administration Client on Microsoft Windows 10
Write and Encrypt
Read and Unencrypt
PKCS#11
nCipher nShield Connect HSMs
Bloombase StoreSafe
NFS, SMB, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
\\storage01\smb01
storage01:/nfs01
iqn.1991-05.com.microsoft:iscsi01
^$8Yn +=@~
Windows Server
Microsoft Storage Server on Microsoft Windows Server 2019

Hardware Security Module

Hardware Security Module	nCipher nShield Connect XC HSMs v12.60.2
Client Software	nCipher nCSS v12.60.11 Security World Software for Linux 64-bit

Remote Administration

Remote Administration	nShield Remote Administration Client and Remote Administration Cards
Client	Microsoft Windows 10

Storage Encryption

Bloombase StoreSafe	Bloombase StoreSafe Intelligent Storage Firewall Software Appliance v3.4.7.13
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

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 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

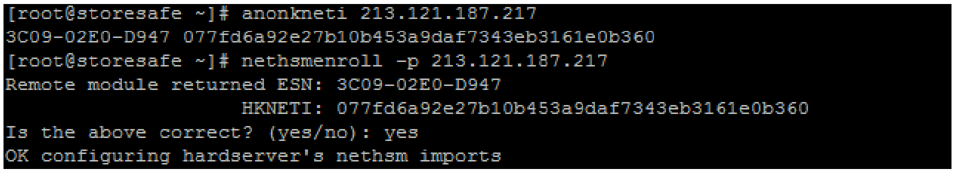
The nCipher nShield Connect HSM is installed with network settings provisioned. In this integration as an example, the nCipher nShield Connect HSM is provided with IP address and Security World. The provided Security World files should be placed in the

`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.



```
[root@storesafe ~]# anonkneti 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
```

In this integration, 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.

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.
```

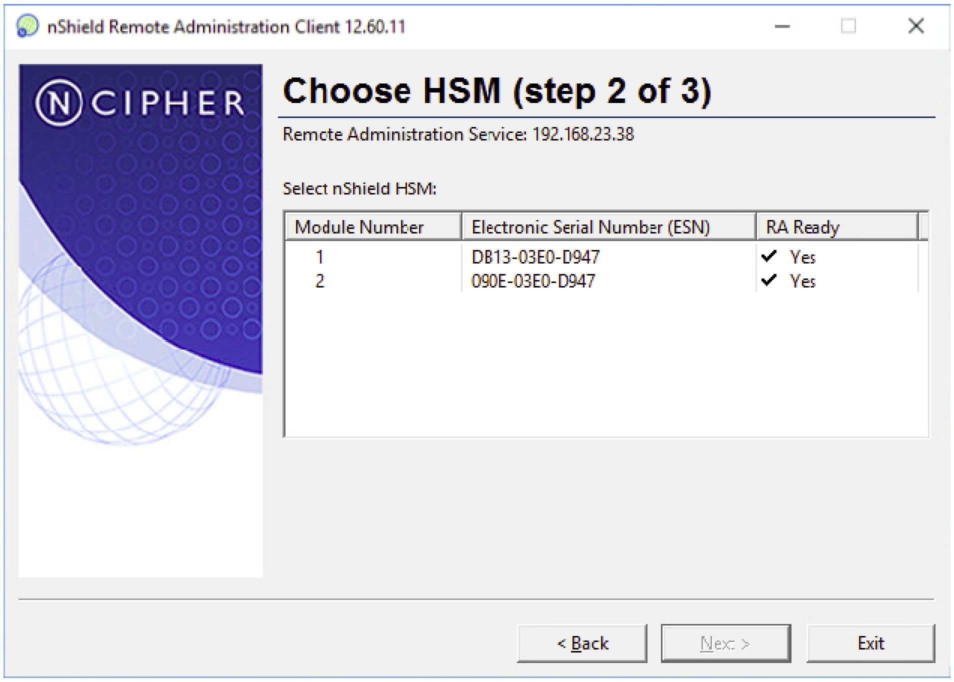
nCipher nShield Remote Administration

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.



Choose HSM (step 2 of 3)

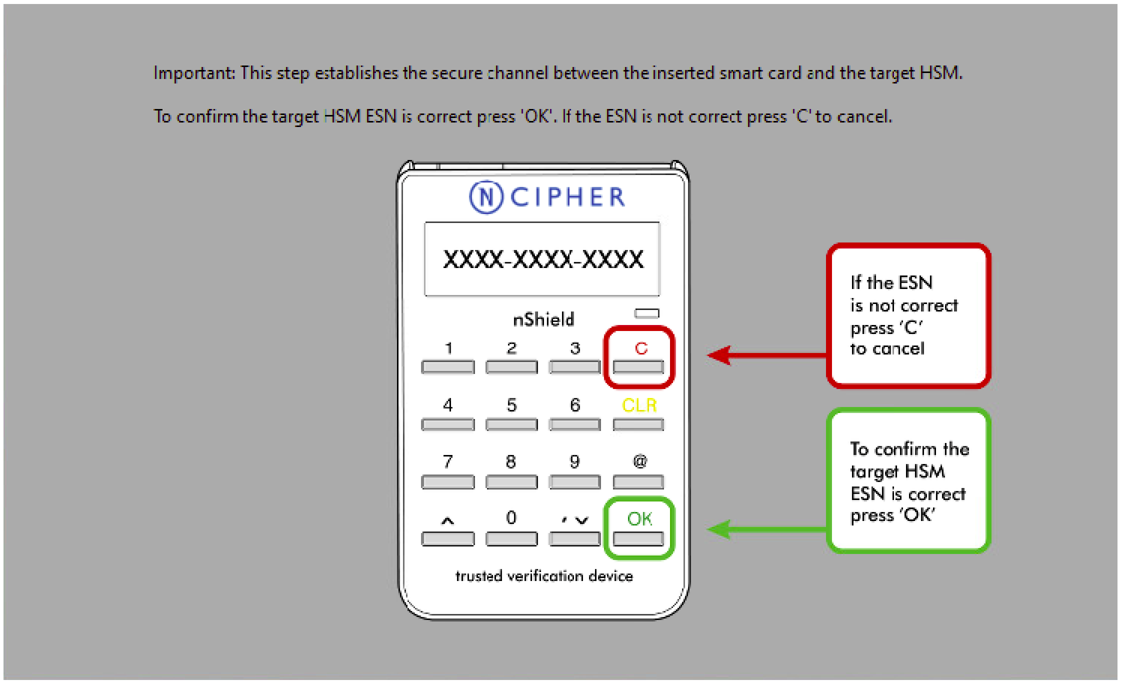
Remcte Administration Service: 192.168.23.38

Select nShield HSM:

Module Number	Electronic Serial Number (ESN)	RA Ready
1	DB13-03E0-D947	✓ Yes
2	090E-03E0-D947	✓ Yes

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.



Important: This step establishes the secure channel between the inserted smart card and the target HSM.

To confirm the target HSM ESN is correct press 'OK'. If the ESN is not correct press 'C' to cancel.

If the ESN is not correct press 'C' to cancel

To confirm the target HSM ESN is correct press 'OK'

nShield Remote Administration Cards Initialization and Operations

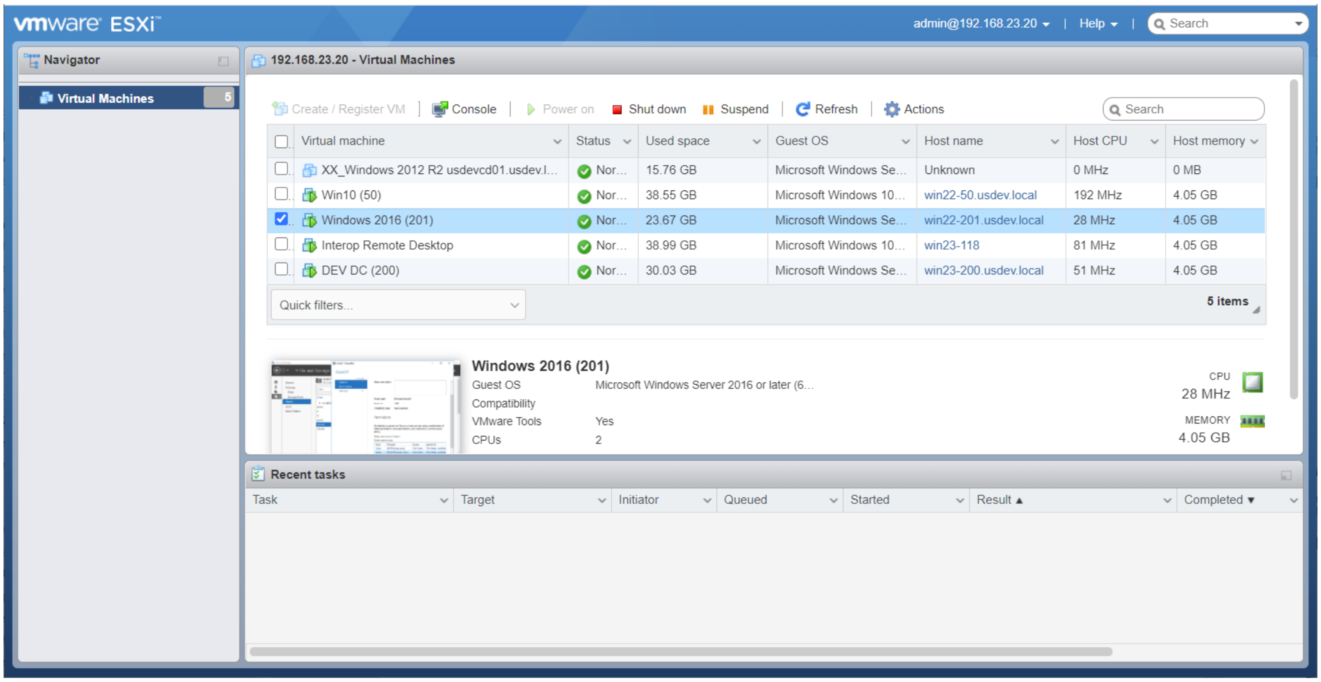
Use the following command on a blank card inserted into the Trusted Verification Device (TVD) to create the operator cardset.

```
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.


vmware ESXi
admin@192.168.23.20 | Help | Search
Navigator
Virtual Machines 5
192.168.23.20 - Virtual Machines
Create / Register VM | Console | Power on | Shut down | Suspend | Refresh | Actions
Search
Quick filters...
Recent tasks

☐	Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory
☐	XX_Windows 2012 R2 usdevcd01.usdev.l...	Nor...	15.76 GB	Microsoft Windows Se...	Unknown	0 MHz	0 MB
☐	Win10 (50)	Nor...	38.55 GB	Microsoft Windows 10...	win22-50.usdev.local	192 MHz	4.05 GB
☑	Windows 2016 (201)	Nor...	23.67 GB	Microsoft Windows Se...	win22-201.usdev.local	28 MHz	4.05 GB
☐	Interop Remote Desktop	Nor...	38.99 GB	Microsoft Windows 10...	win23-118	81 MHz	4.05 GB
☐	DEV DC (200)	Nor...	30.03 GB	Microsoft Windows Se...	win23-200.usdev.local	51 MHz	4.05 GB

5 items

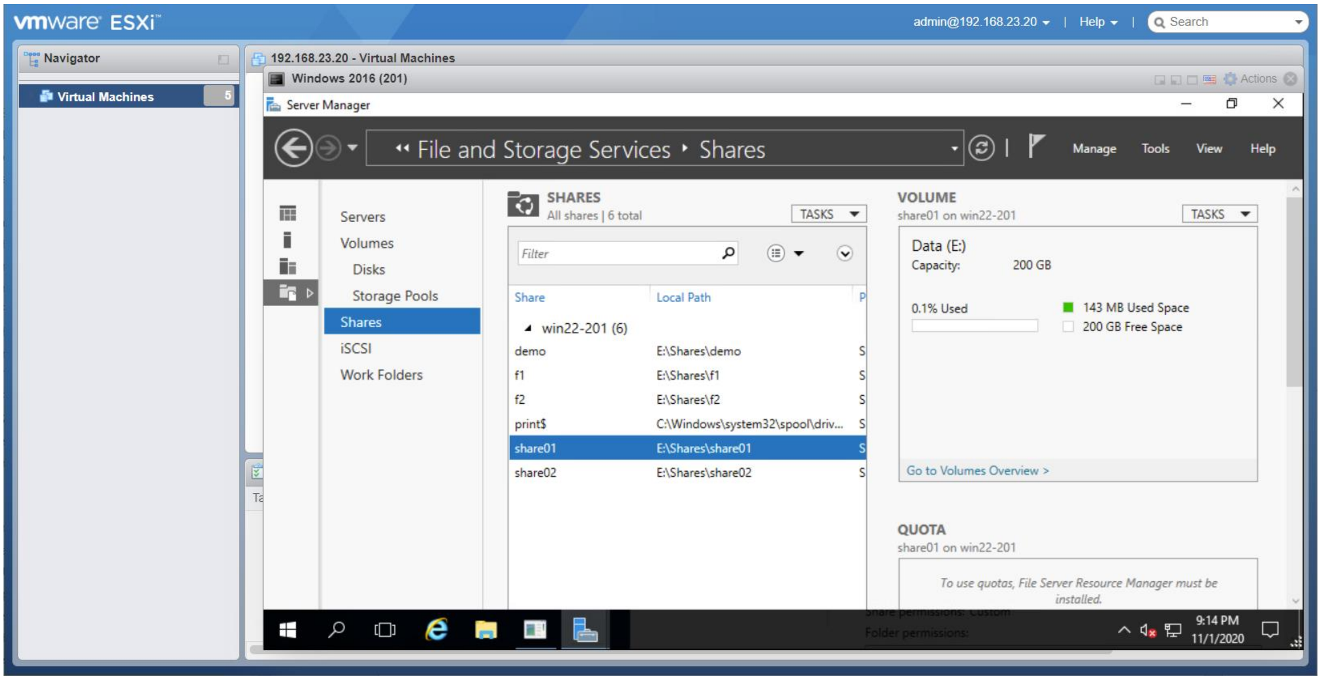
Windows 2016 (201)

Guest OS Microsoft Windows Server 2016 or later (6...
Compatibility
VMware Tools Yes
CPUs 2

CPU 28 MHz
MEMORY 4.05 GB

Task	Target	Initiator	Queued	Started	Result ▲	Completed ▼

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



SHARES
All shares | 6 total

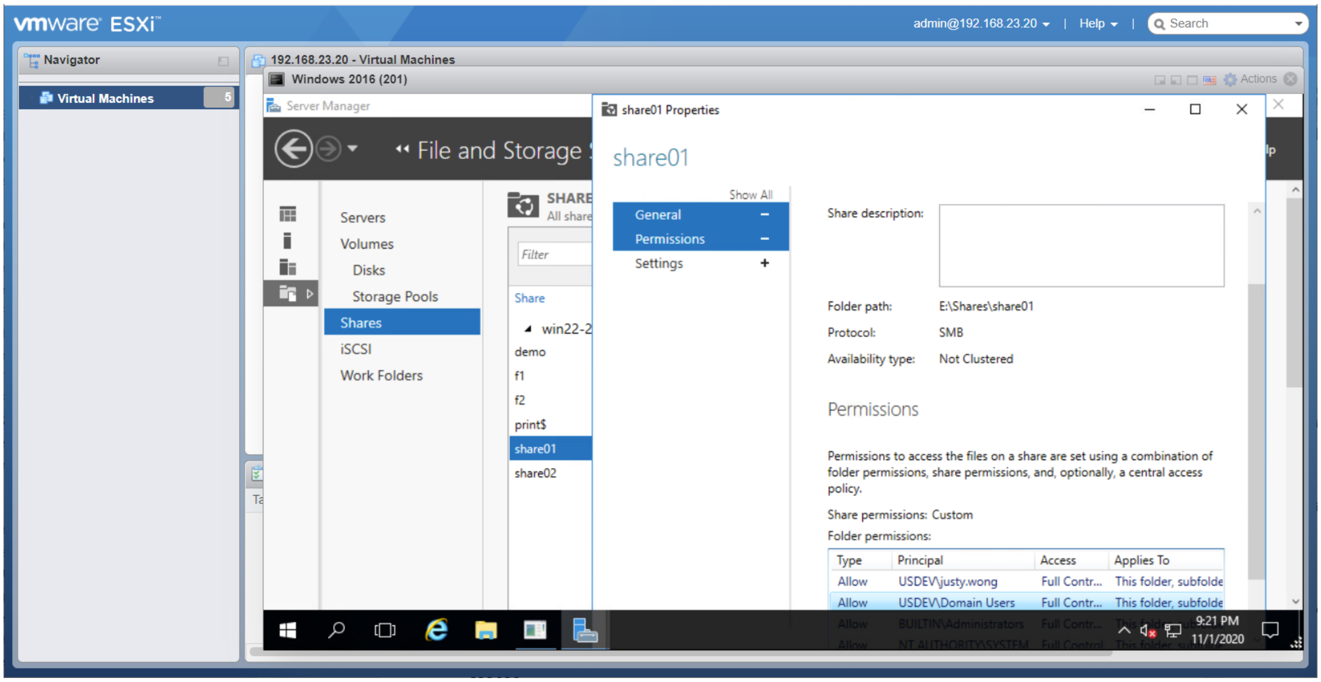
Share	Local Path
win22-201 (6)	
demo	E:\Shares\demo
f1	E:\Shares\f1
f2	E:\Shares\f2
print$	C:\Windows\system32\spool\driv...
share01	E:\Shares\share01
share02	E:\Shares\share02

VOLUME
share01 on win22-201

Data (E:)
Capacity: 200 GB
0.1% Used
143 MB Used Space
200 GB Free Space

QUOTA
share01 on win22-201

To use quotas, File Server Resource Manager must be installed.



Share description:

Folder path: E:\Shares\share01

Protocol: SMB

Availability type: Not Clustered

Permissions

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Custom

Folder permissions:

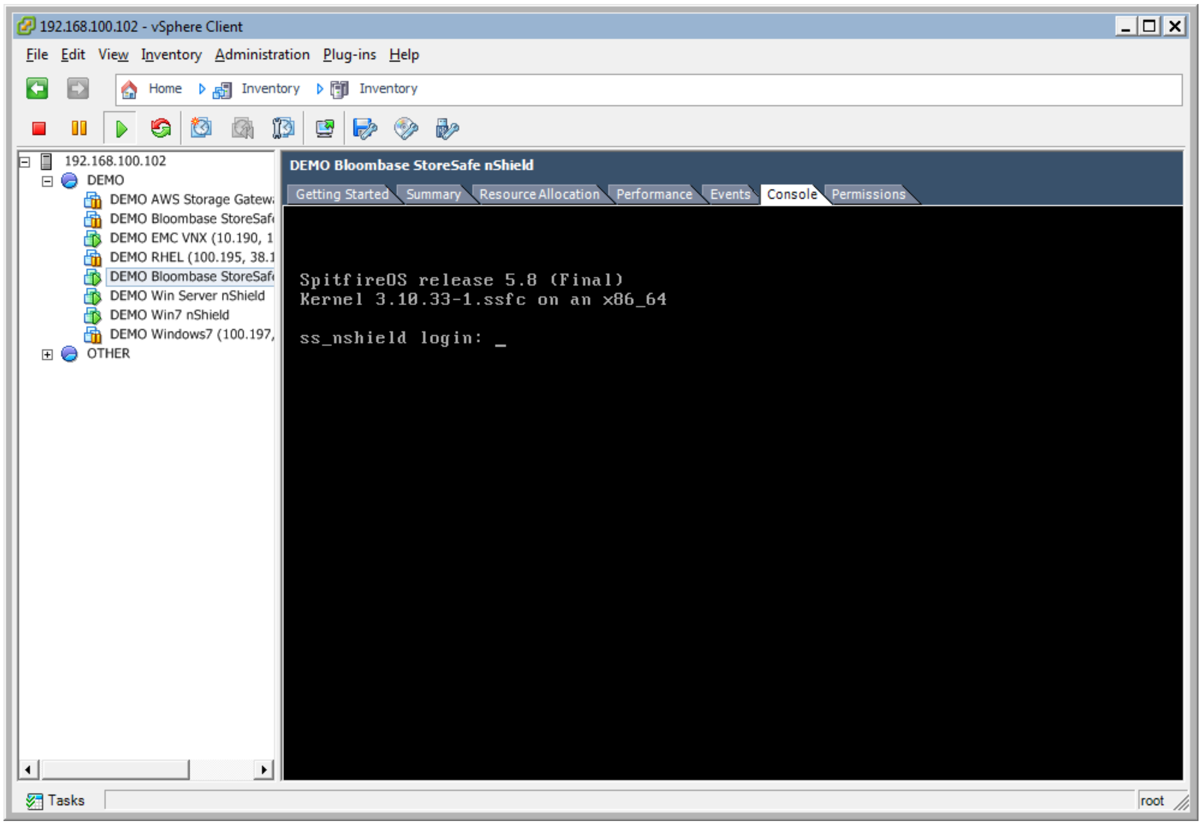
Type	Principal	Access	Applies To
Allow	USDEV\justy.wong	Full Contr...	This folder, subfolde
Allow	USDEV\Domain Users	Full Contr...	This folder, subfolde
Allow	BUILTIN\Administrators	Full Contr...	This folder, subfolde
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolde

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

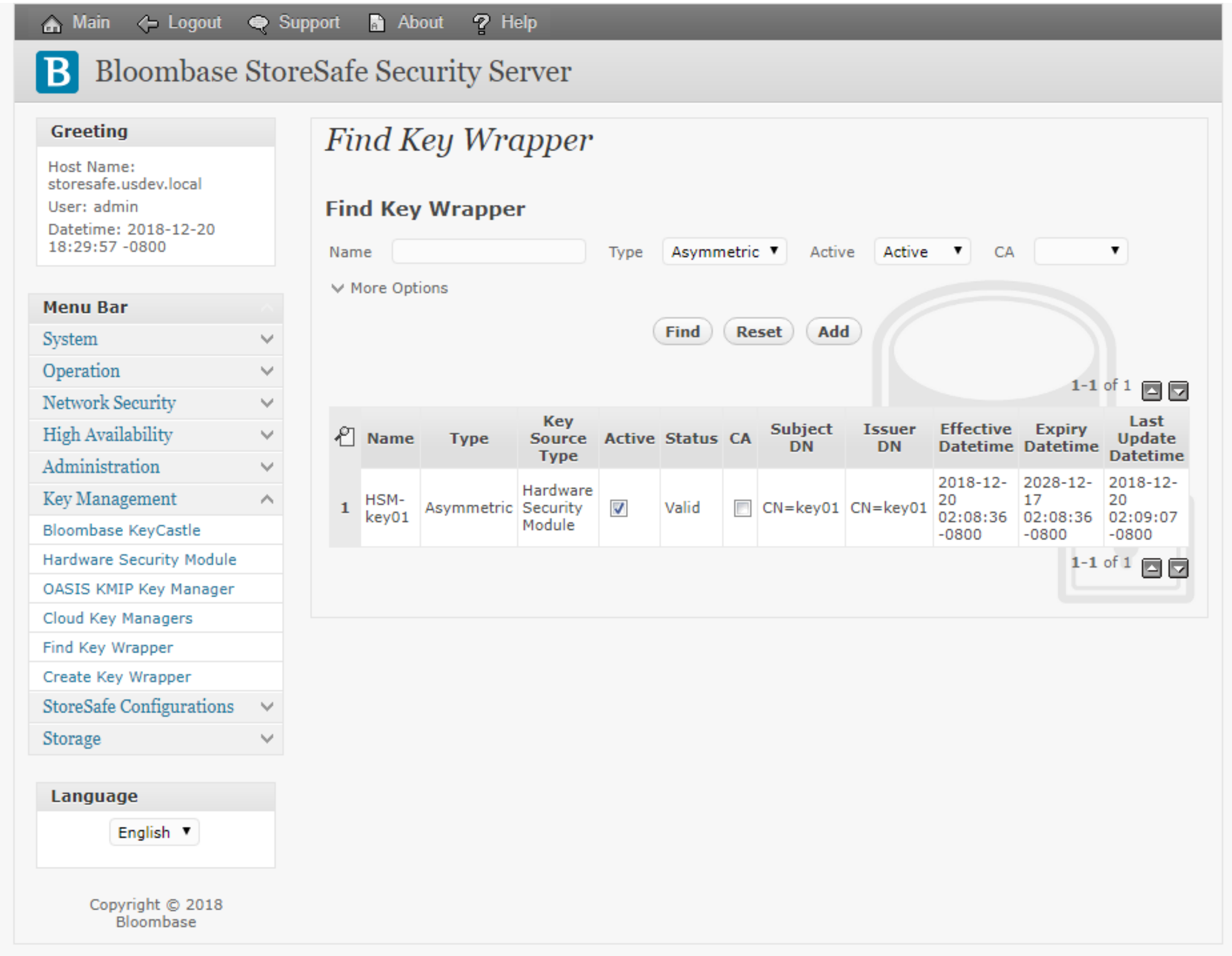
Bloombase StoreSafe delivers unified data at-rest encryption security of files, block devices, objects, sequential storages, etc. In this interoperability test, file-based encryption security service is validated against Bloombase StoreSafe with keys managed at nCipher nShield Connect HSMs.



```
SpitfireOS release 5.8 (Final)
Kernel 3.10.33-1.ssfc on an x86_64

ss_nshield login: _
```

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



Host Name: storesafe.usdev.local
User: admin
Datetime: 2018-12-20 18:29:57 -0800

Find Key Wrapper

Find Key Wrapper

Name: Type: Asymmetric Active: Active CA:

	Name	Type	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1	HSM-key01	Asymmetric	Hardware Security Module	☑	Valid	□	CN=key01	CN=key01	2018-12-20 02:08:36 -0800	2028-12-17 02:08:36 -0800	2018-12-20 02:09:07 -0800

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

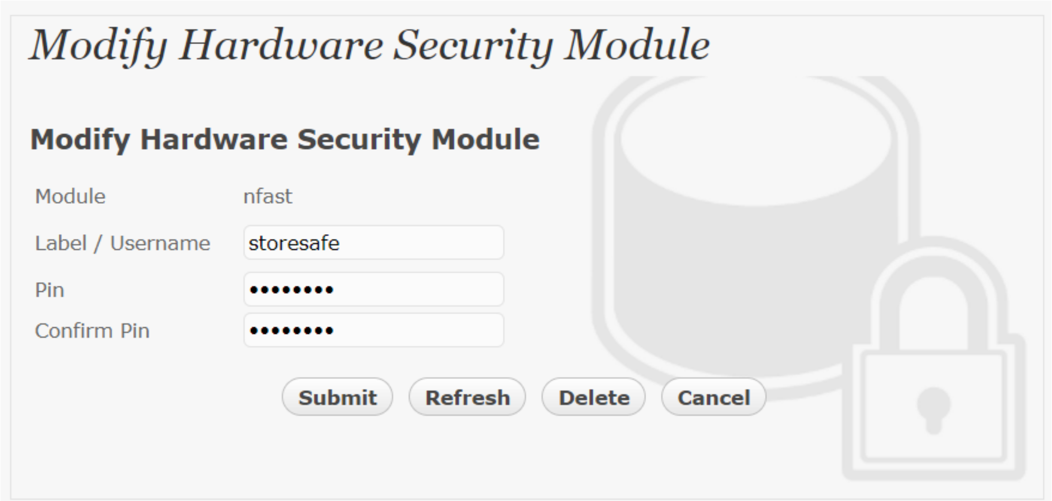
```
slotListIndex
```

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.



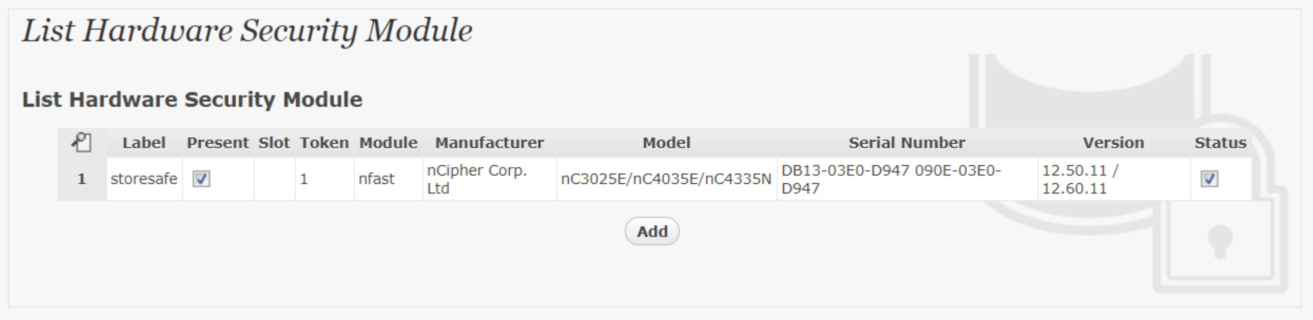
Modify Hardware Security Module

Modify Hardware Security Module

Module	nfast
Label / Username	storesafe
Pin	••••••••
Confirm Pin	••••••••

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	☑		1	nfast	nCipher Corp. Ltd	nC3025E/nC4035E/nC4335N	DB13-03E0-D947 090E-03E0-D947	12.50.11 / 12.60.11	☑

Encryption Key Provisioning

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

```
Hardware Security Module
```

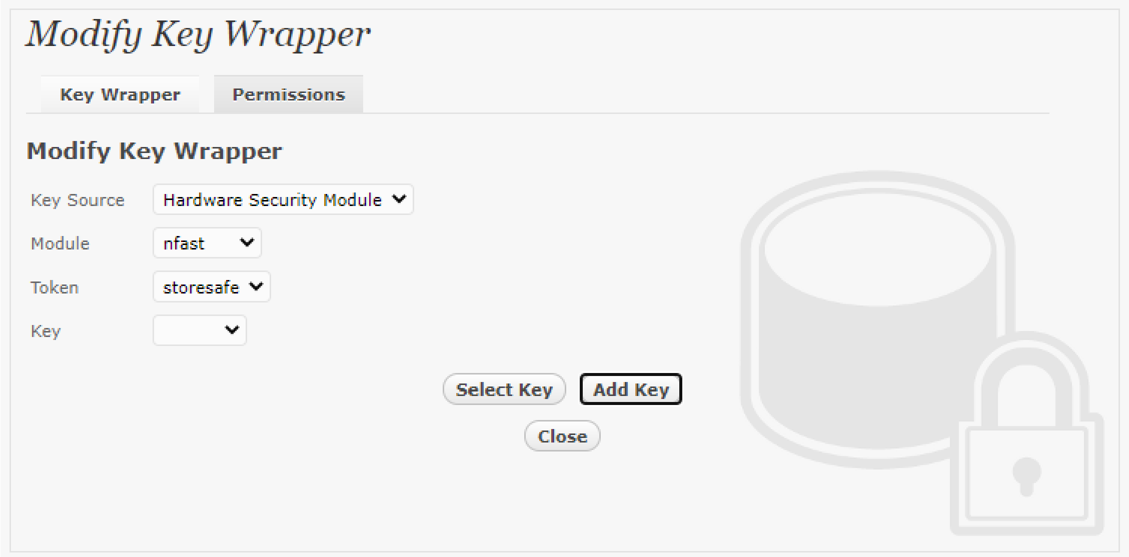
Module as

```
nfast
```

and the assigned HSM token label, in this case

```
storesafe
```

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

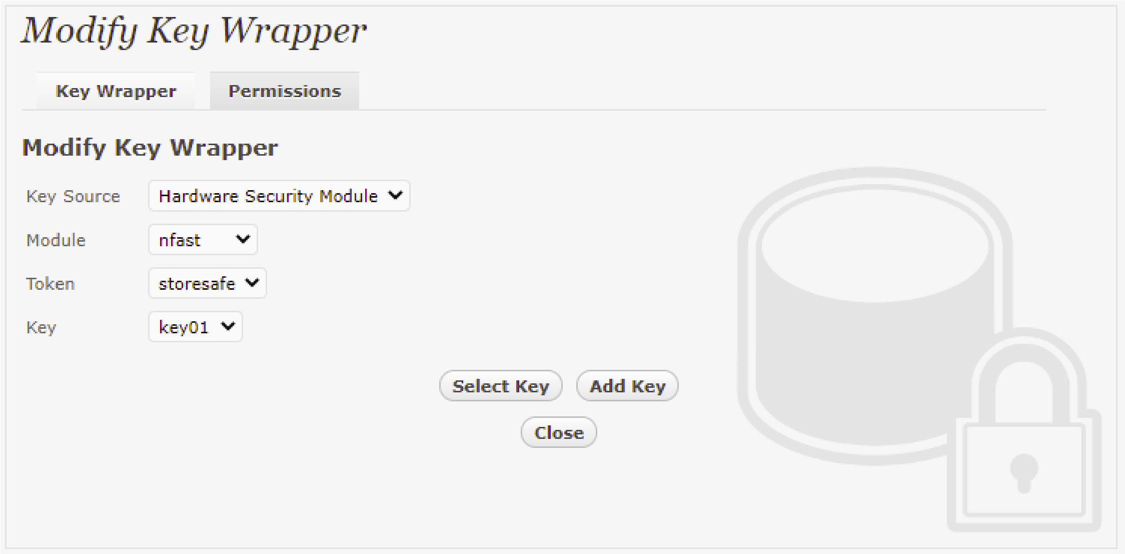


Modify Key Wrapper

Modify Key Wrapper

Key Source: Hardware Security Module
Module: nfast
Token: storesafe
Key:

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



Modify Key Wrapper

Modify Key Wrapper

Key Source: Hardware Security Module
Module: nfast
Token: storesafe
Key: key01

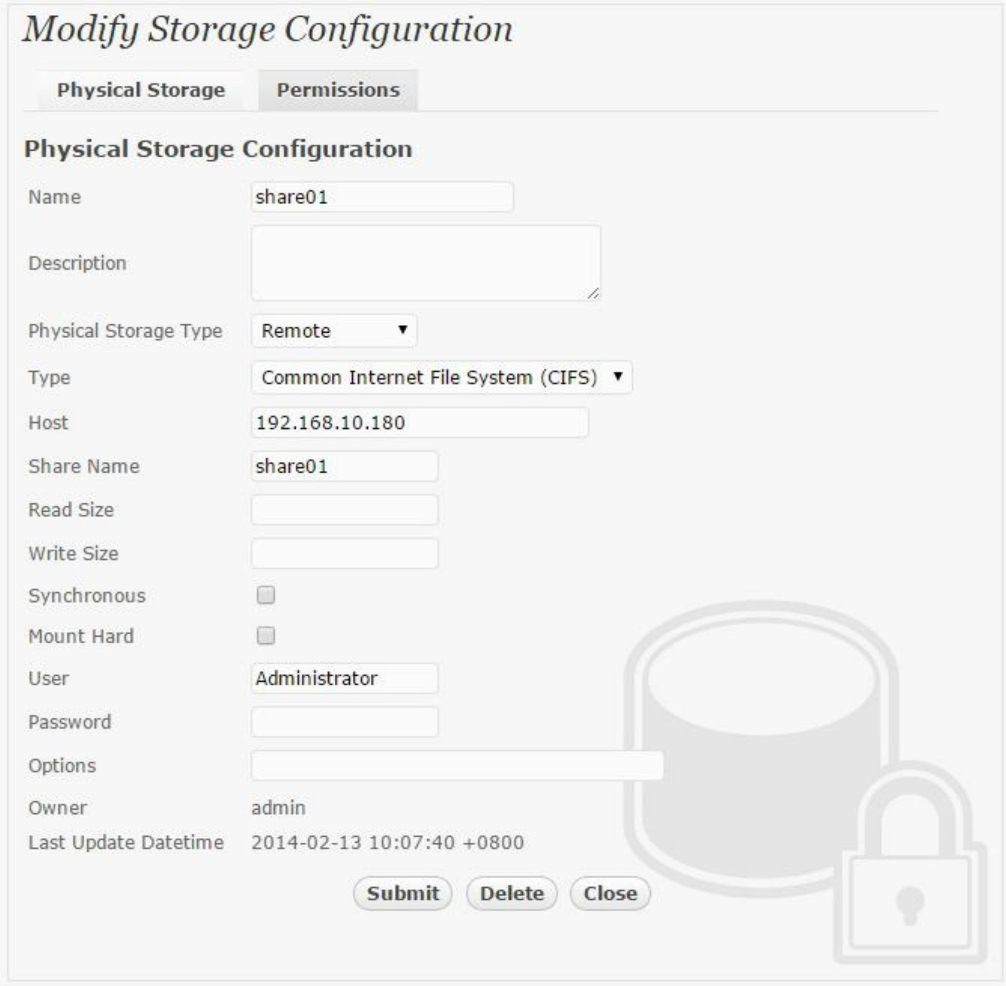
Ensure you import a key from the HSM before you submit the key wrapper.

Backend Physical Storage Configuration

Physical storage namely

```
share01
```

is configured to be secured by Bloombase StoreSafe using encryption.



Modify Storage Configuration

Physical Storage 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	□
Mount Hard	□
User	Administrator
Password	
Options	
Owner	admin
Last Update Datetime	2014-02-13 10:07:40 +0800

Secure Storage Configuration

Virtual storage namely

```
share01
```

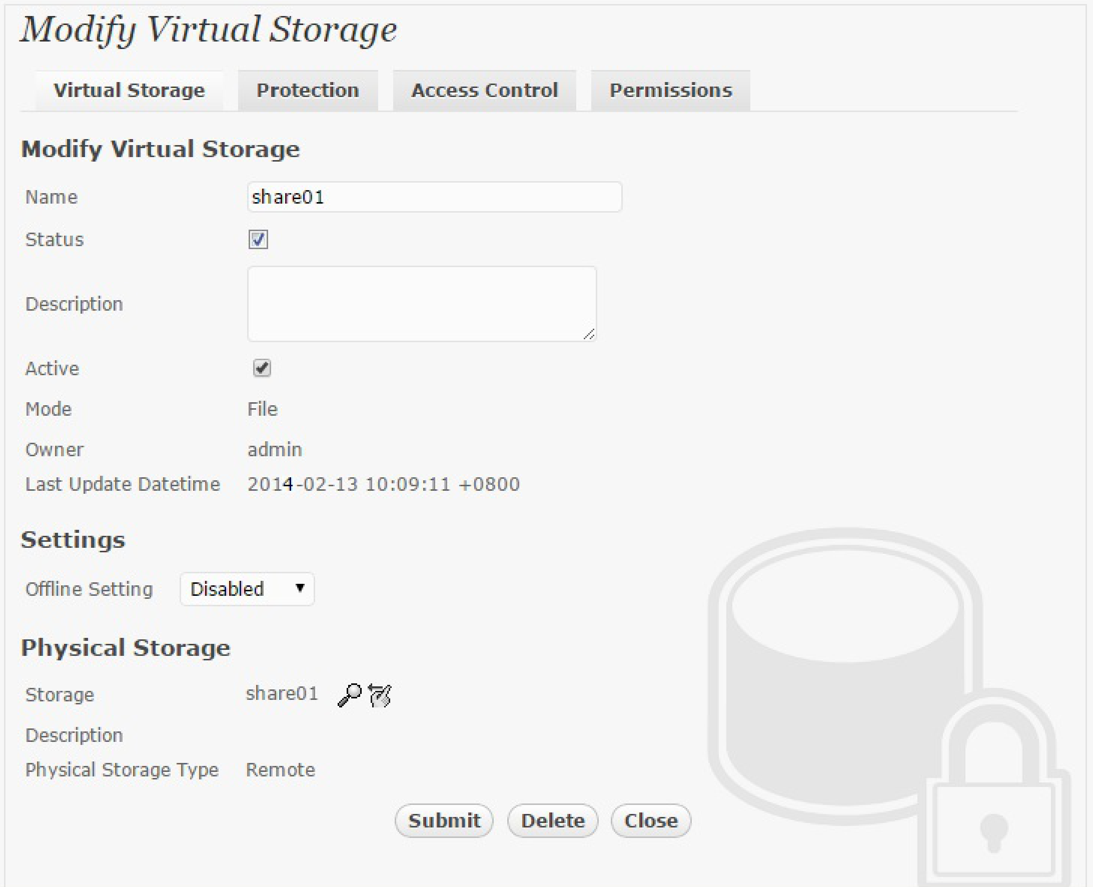
of type

```
File
```

is created to virtualize physical storage

```
share01
```

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



Modify Virtual Storage

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
```

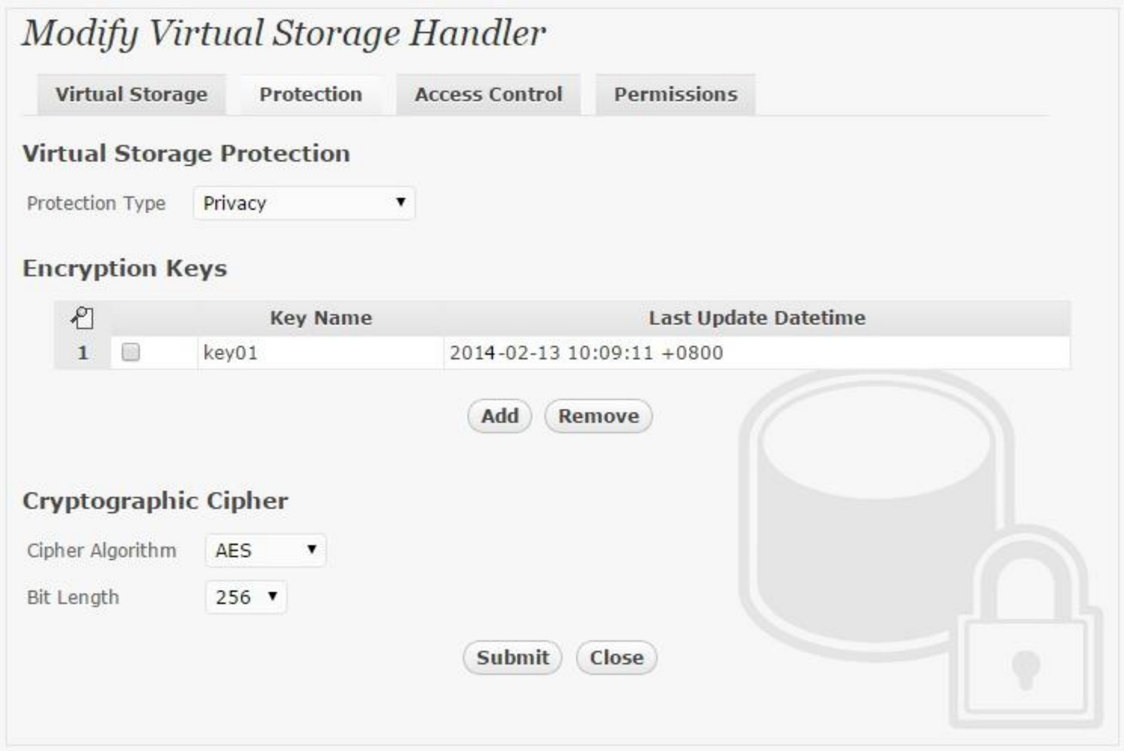
and secure the Microsoft Storage Server storage backend using

```
AES 256-bit
```

encryption and encryption key

```
key01
```

managed at nCipher nShield Connect HSM.



Virtual Storage Protection

Protection Type: Privacy

Encryption Keys

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

Cryptographic Cipher

Cipher Algorithm: AES

Bit Length: 256

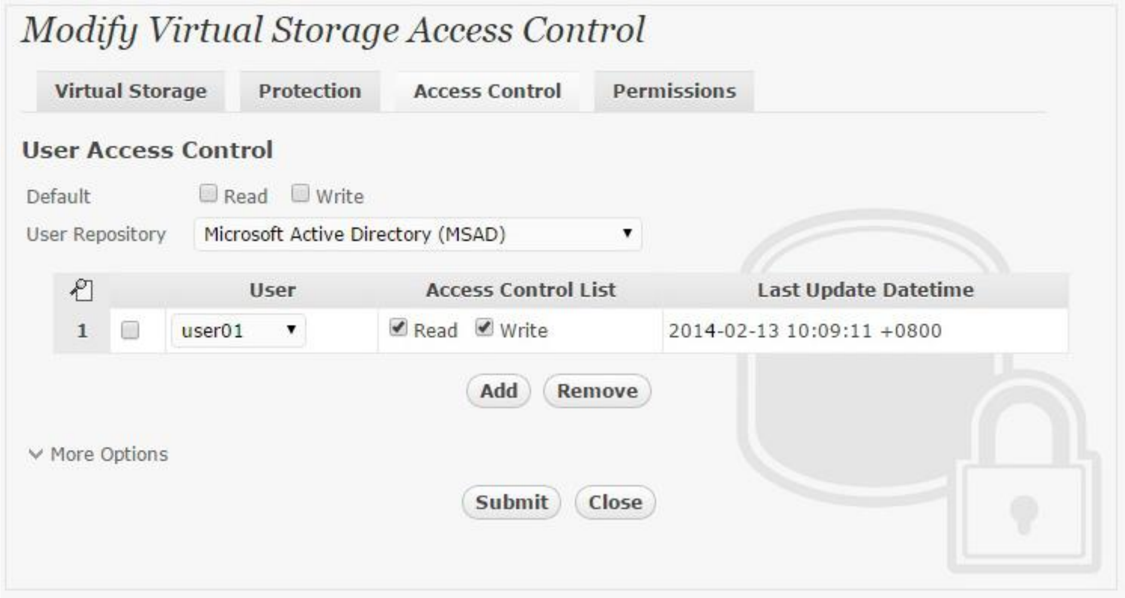
SMB/CIFS storage protocol relies mainly on user-password authentication for access control. In this test, the Bloombase StoreSafe secure storage resource

```
share01
```

is provisioned for user

```
user01
```

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



Modify Virtual Storage Access Control

User Access Control

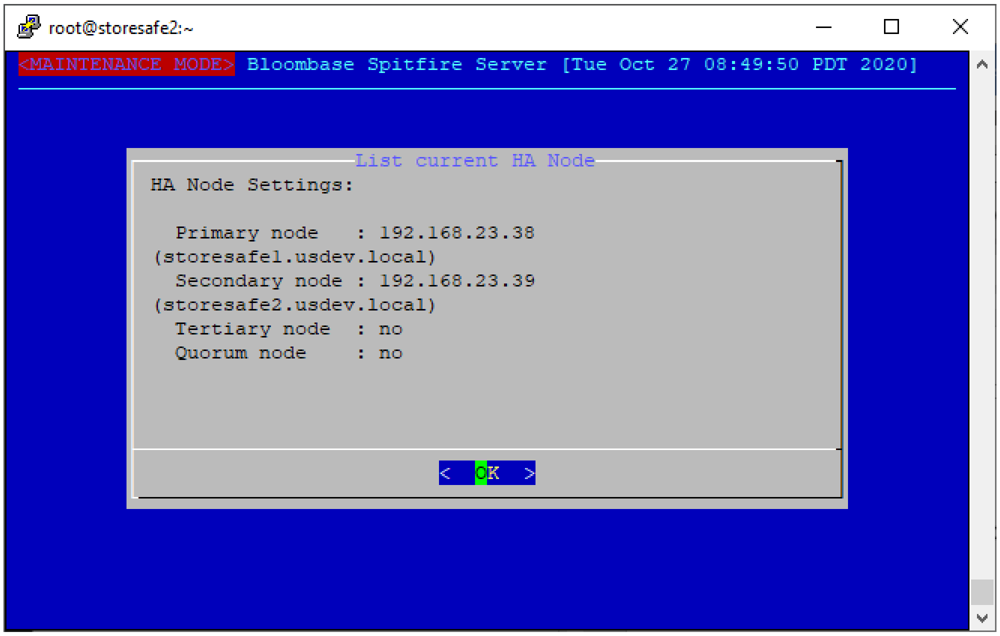
Default □ Read □ Write

User Repository: Microsoft Active Directory (MSAD)

		User	Access Control List	Last Update Datetime
1	□	user01	☑ Read ☑ Write	2014-02-13 10:09:11 +0800

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.



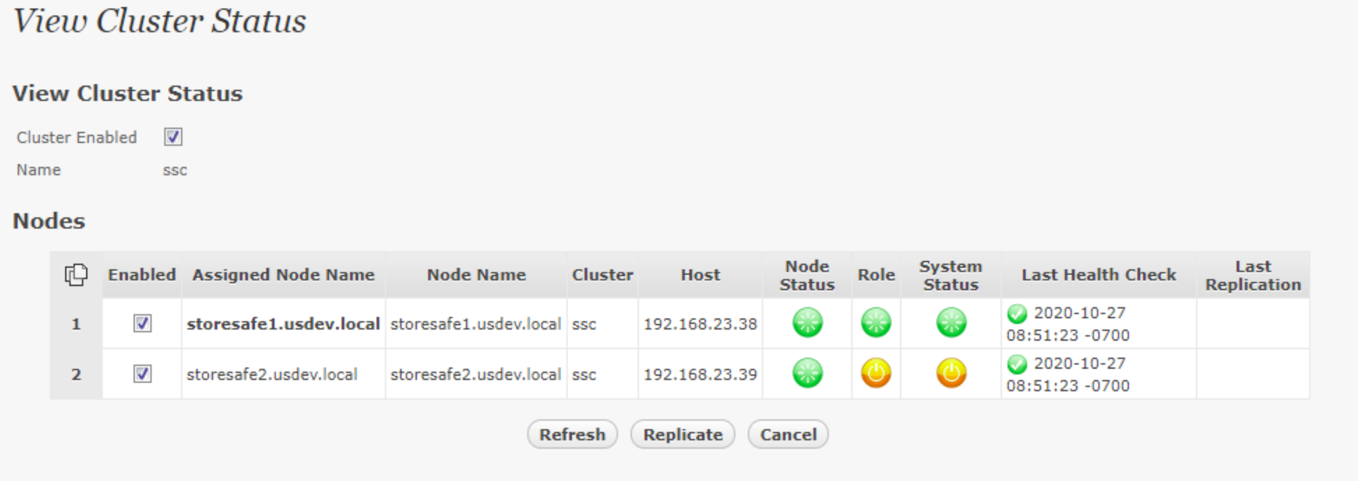
```
<MAINTENANCE MODE> Bloombase Spitfire Server [Tue Oct 27 08:49:50 PDT 2020]

List current HA Node
HA Node Settings:

  Primary node   : 192.168.23.38
(storesafe1.usdev.local)
  Secondary node : 192.168.23.39
(storesafe2.usdev.local)
  Tertiary node  : no
  Quorum node    : no

< OK >
```

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 ssc

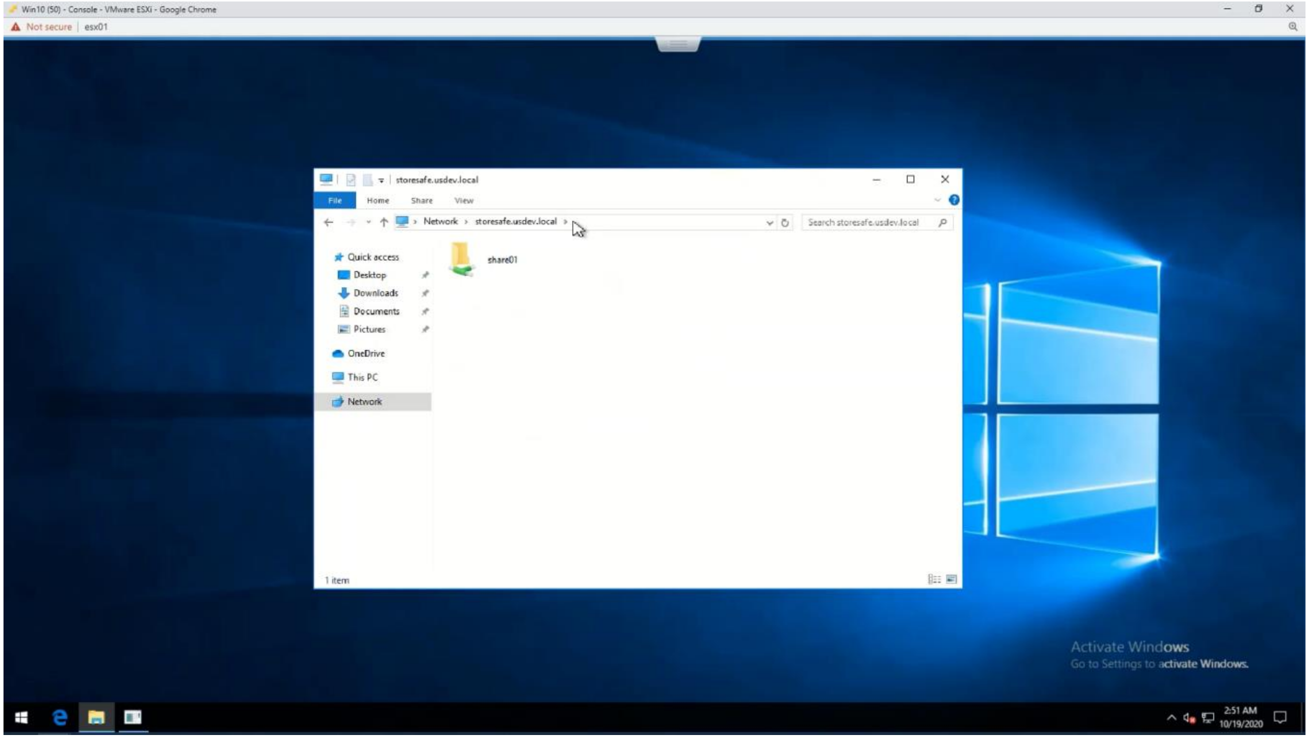
Nodes

	Enabled	Assigned Node Name	Node Name	Cluster	Host	Node Status	Role	System Status	Last Health Check	Last Replication
1	☑	**storesafe1.usdev.local**	storesafe1.usdev.local	ssc	192.168.23.38	🟢	🟢	🟢	✓ 2020-10-27 08:51:23 -0700	
2	☑	storesafe2.usdev.local	storesafe2.usdev.local	ssc	192.168.23.39	🟢	🟡	🟡	✓ 2020-10-27 08:51:23 -0700	

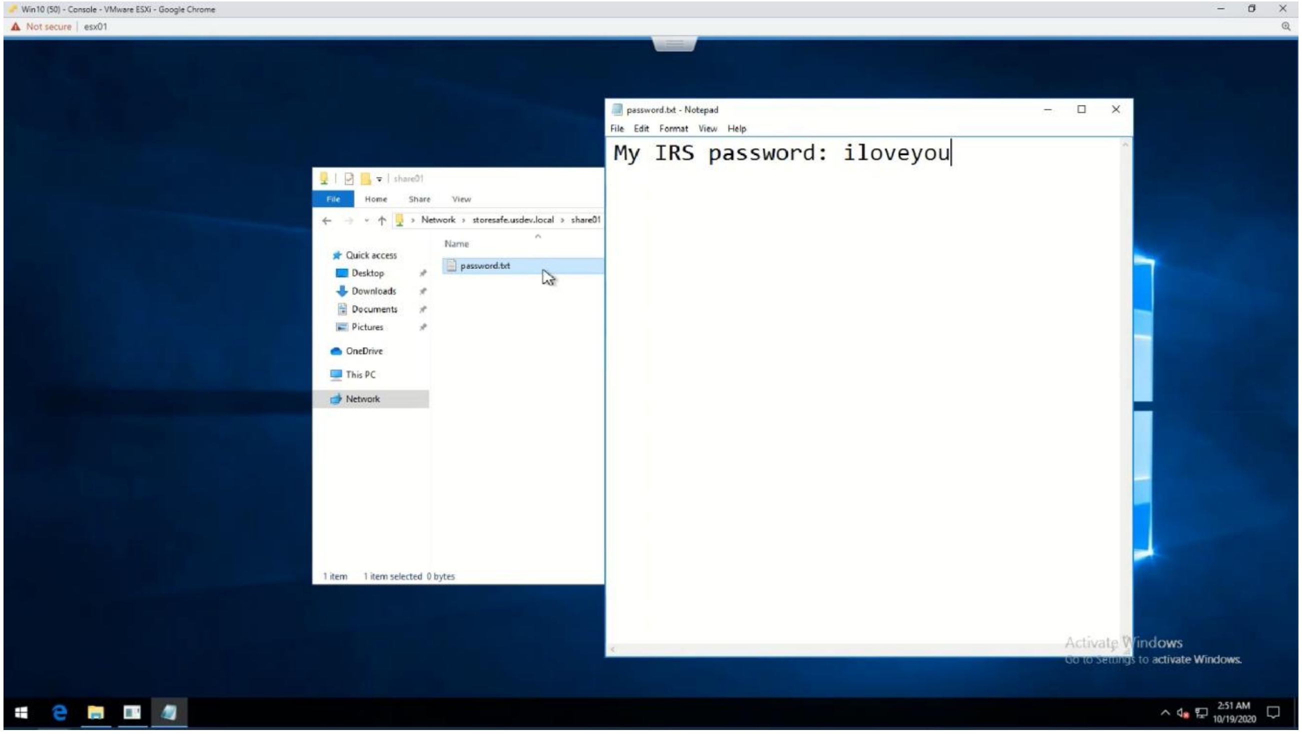
Use Case

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.

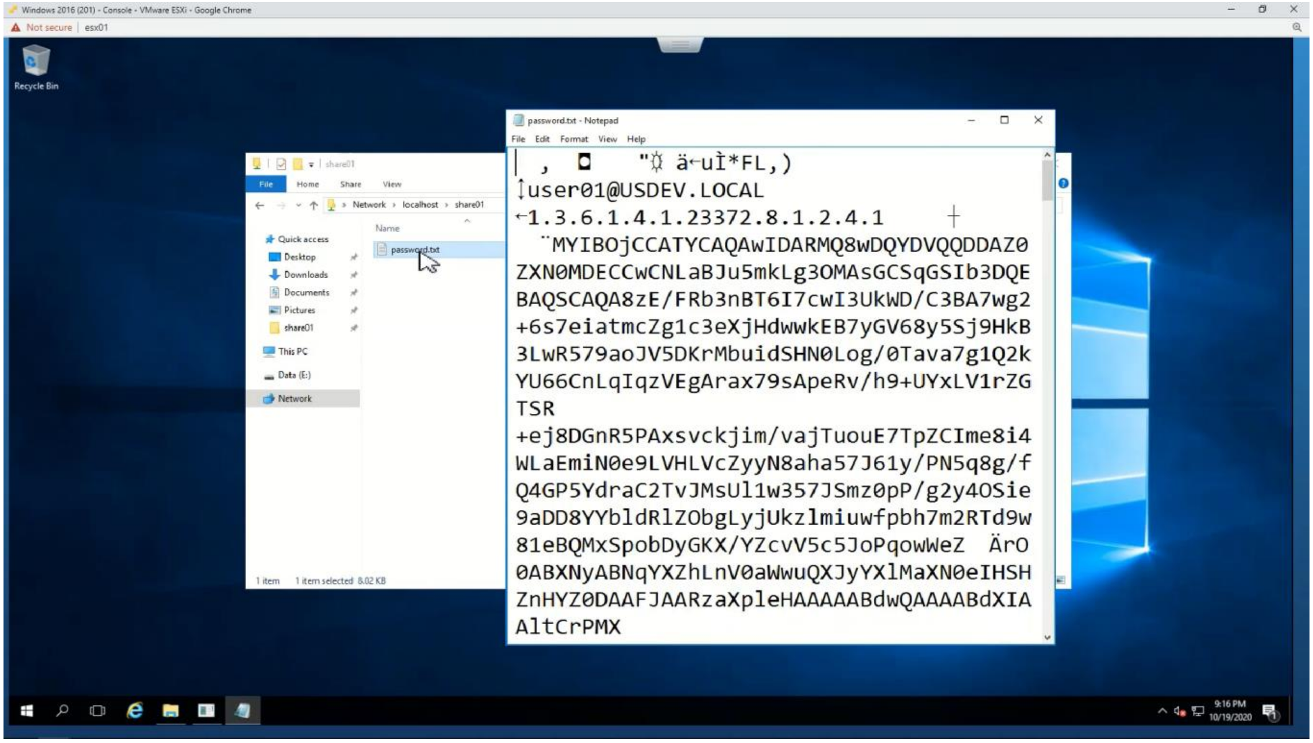


On the demo virtual encrypted SMB share, a sample plaintext file is created by the client and saved. The file is transparently encrypted by the Bloombase StoreSafe encryption engine and stored on the Windows Server 2019 backend share.



```
My IRS password: iloveyou
```

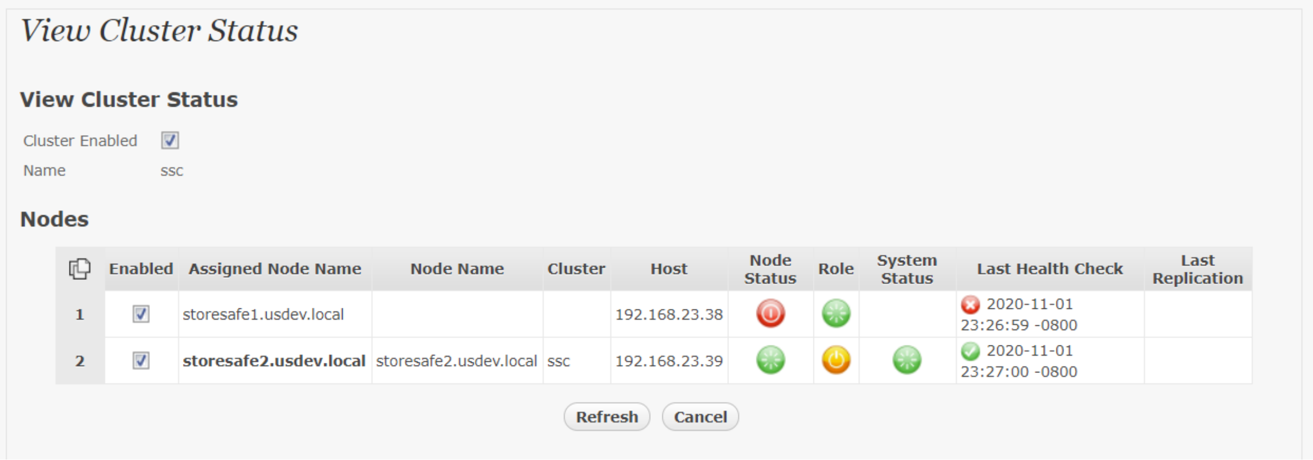
If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.



```
 ,  ◘   "☼ ä←uÌ*FL,)
↕user01@USDEV.LOCAL
←1.3.6.1.4.1.23372.8.1.2.4.1
  ¨MYIBOjCCATYCAQAwIDARMQ8wDQYDVQQDDAZ0
ZXN0MDECCwCNLaBJu5mkLg3OMAsGCSqGSIb3DQE
BAQSCAQA8zE/FRb3nBT6I7cwI3UkWD/C3BA7wg2
+6s7eiatmcZg1c3eXjHdwwkEB7yGV68y5Sj9HkB
3LwR579aoJV5DKrMbuidSHN0Log/0Tava7g1Q2k
YU66CnLqIqzVEgArax79sApeRv/h9+UYxLV1rZG
TSR
+ej8DGnR5PAxsvckjim/vajTuouE7TpZCIme8i4
WLaEmiN0e9LVHLVcZyyN8aha57J61y/PN5q8g/f
Q4GP5YdraC2TvJMsUl1w357JSmz0pP/g2y4OSie
9aDD8YYbldRlZObgLyjUkzlmiuwfpbh7m2RTd9w
81eBQMxSpobDyGKX/YZcvV5c5JoPqowWeZ  ÄrO
0ABXNyABNqYXZhLnV0aWwuQXJyYXlMaXN0eIHSH
ZnHYZ0DAAFJAARzaXpleHAAAAABdwQAAAABdXIA
AltCrPMX
```

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

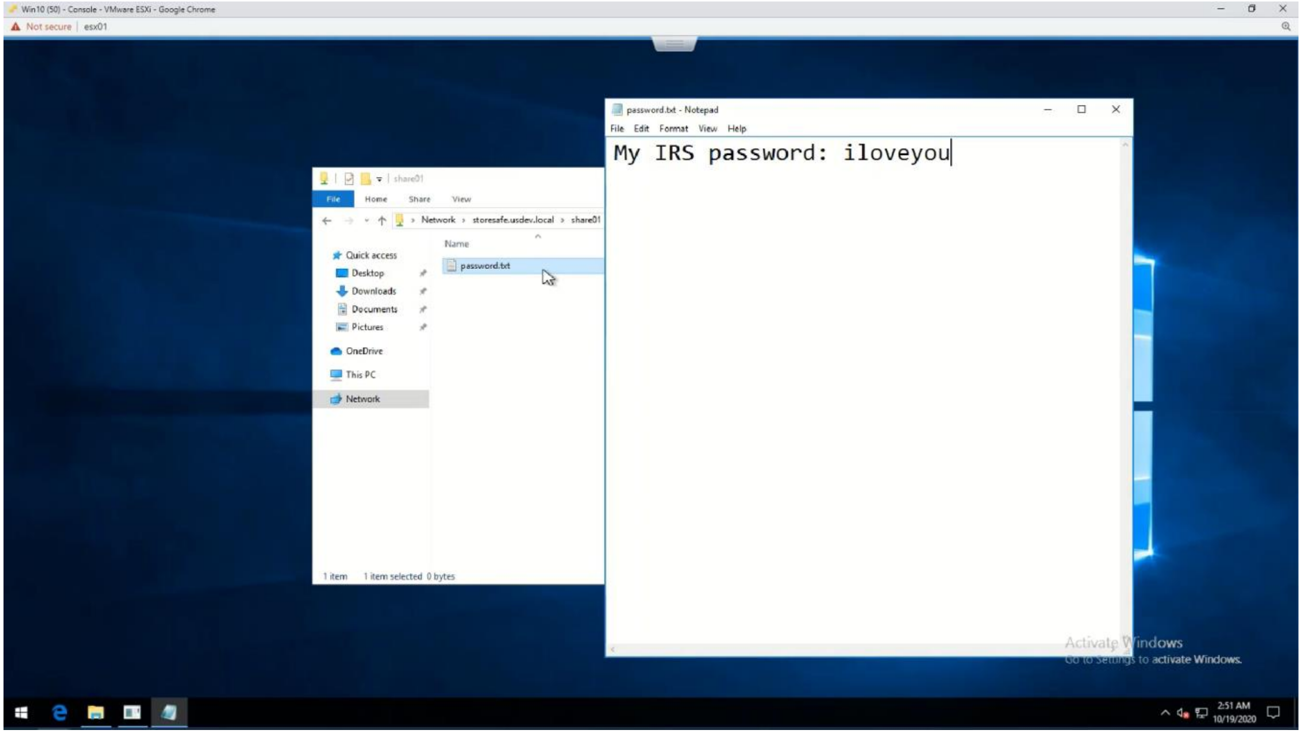
View Cluster Status

Cluster Enabled ☑
Name ssc

Nodes

	Enabled	Assigned Node Name	Node Name	Cluster	Host	Node Status	Role	System Status	Last Health Check	Last Replication
1	☑	storesafe1.usdev.local			192.168.23.38	●	●		☒ 2020-11-01 23:26:59 -0800	
2	☑	**storesafe2.usdev.local**	storesafe2.usdev.local	ssc	192.168.23.39	●	●	●	✓ 2020-11-01 23:27:00 -0800	

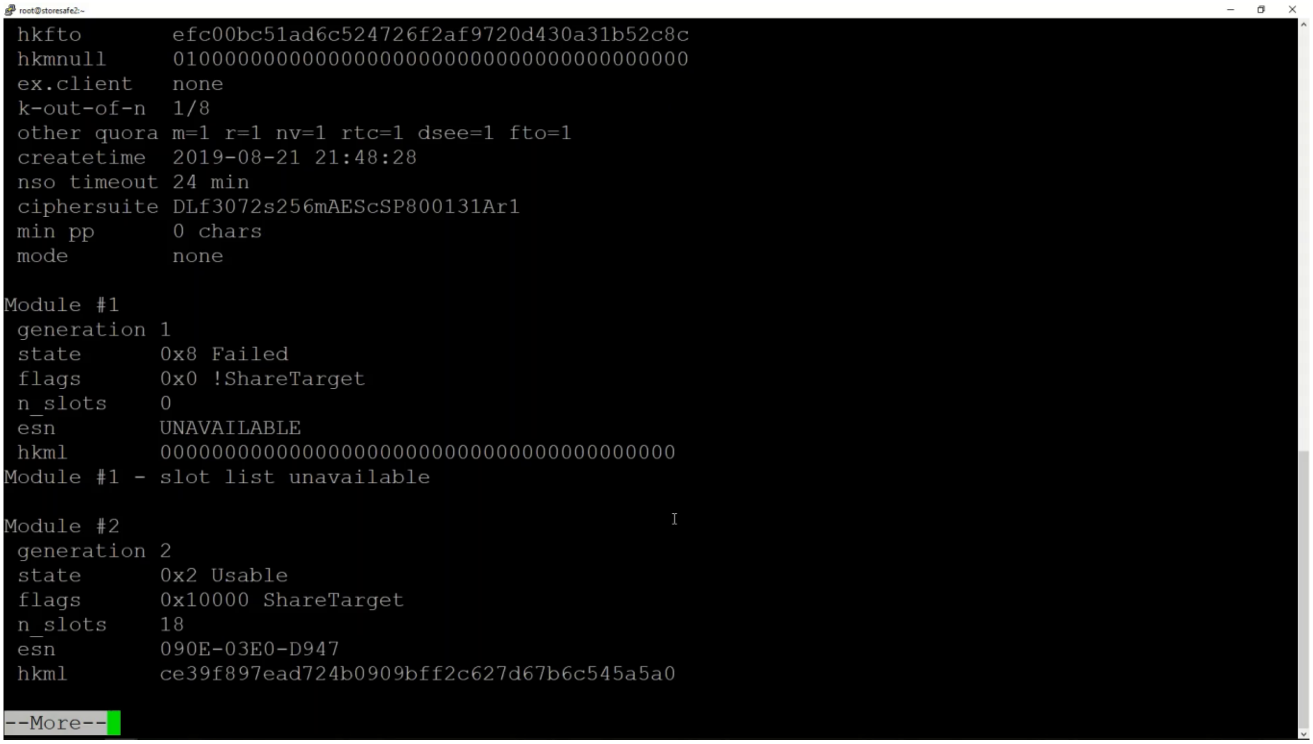
From the client application perspective, no changes have been made. Besides a short interruption in the SMB share during failover, the file share path and data integrity are maintained.



My IRS password: iloveyou

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.



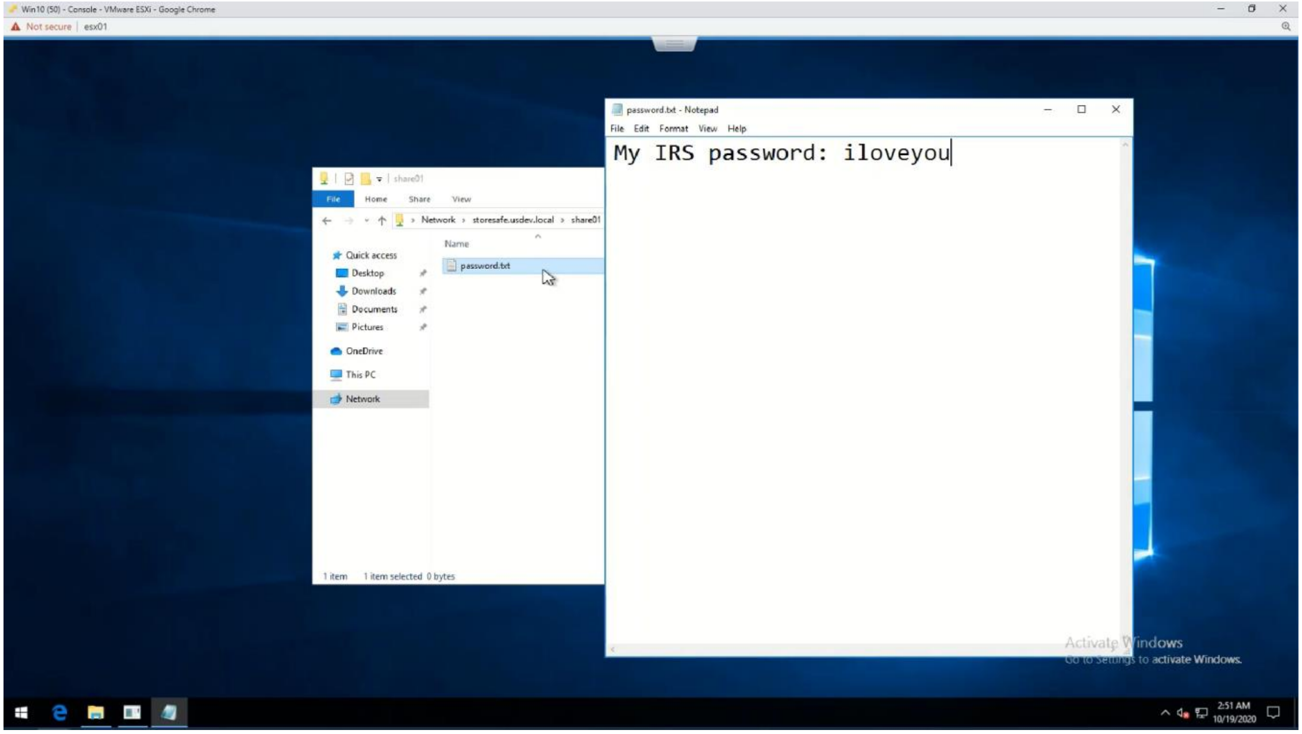
```
 hkfto        efc00bc51ad6c524726f2af9720d430a31b52c8c
 hkmnull      0100000000000000000000000000000000000000
 ex.client    none
 k-out-of-n   1/8
 other quora m=1 r=1 nv=1 rtc=1 dsee=1 fto=1
 createtime   2019-08-21 21:48:28
 nso timeout 24 min
 ciphersuite DLf3072s256mAEScSP800131Ar1
 min pp       0 chars
 mode         none

Module #1
 generation 1
 state       0x8 Failed
 flags       0x0 !ShareTarget
 n_slots     0
 esn         UNAVAILABLE
 hkml        0000000000000000000000000000000000000000
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--
```

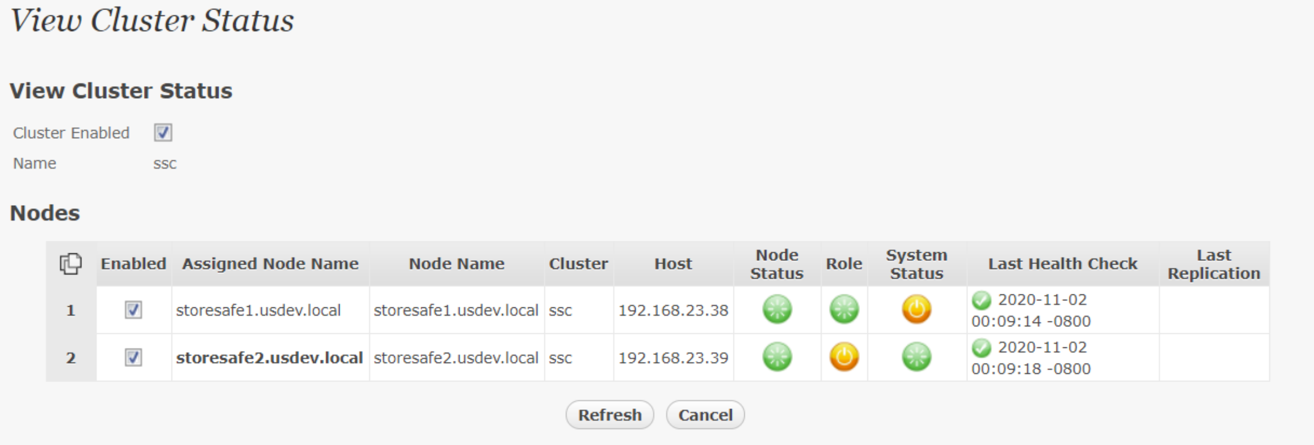
The data encryption process will not have any interruption due to key caching. A new key generation or change to key configuration may be delayed during the timeout period.



My IRS password: iloveyou

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

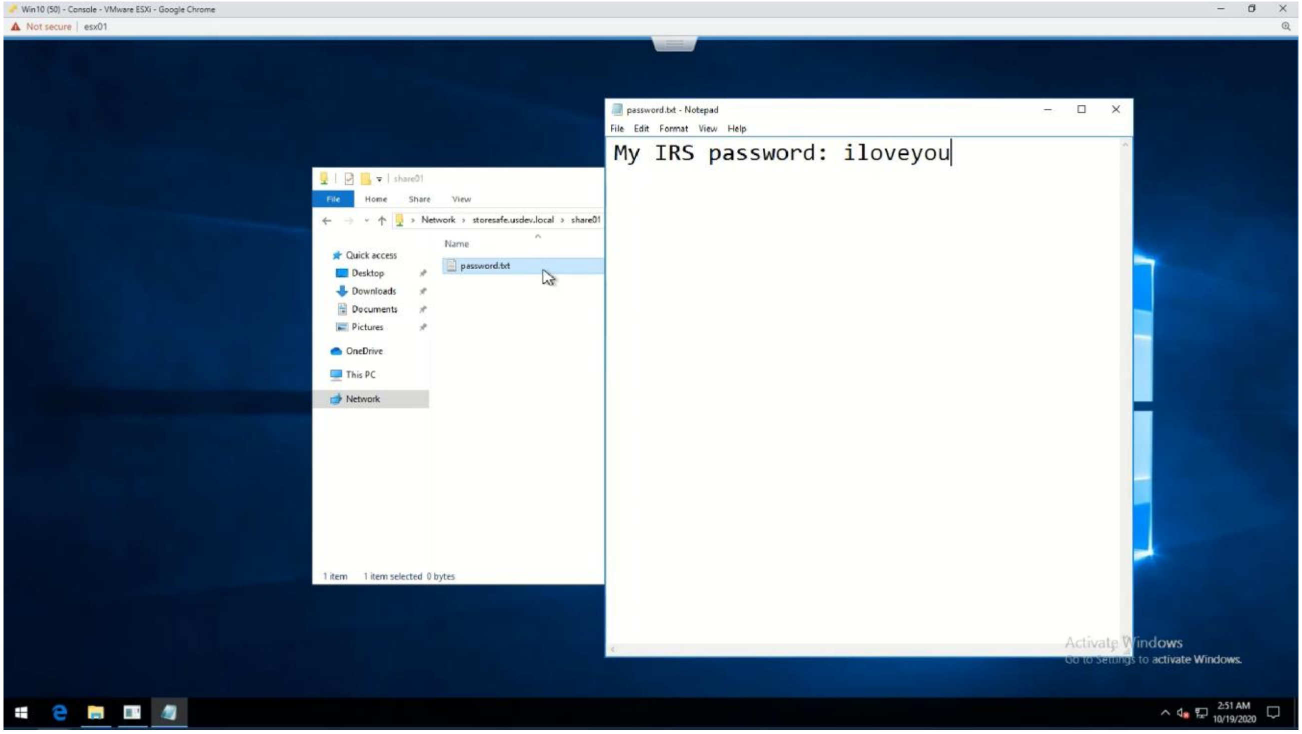
Cluster Enabled ☑

Name ssc

Nodes

	Enabled	Assigned Node Name	Node Name	Cluster	Host	Node Status	Role	System Status	Last Health Check	Last Replication
1	☑	storesafe1.usdev.local	storesafe1.usdev.local	ssc	192.168.23.38	●	●	⏻	✓ 2020-11-02 00:09:14 -0800	
2	☑	**storesafe2.usdev.local**	storesafe2.usdev.local	ssc	192.168.23.39	●	⏻	●	✓ 2020-11-02 00:09:18 -0800	

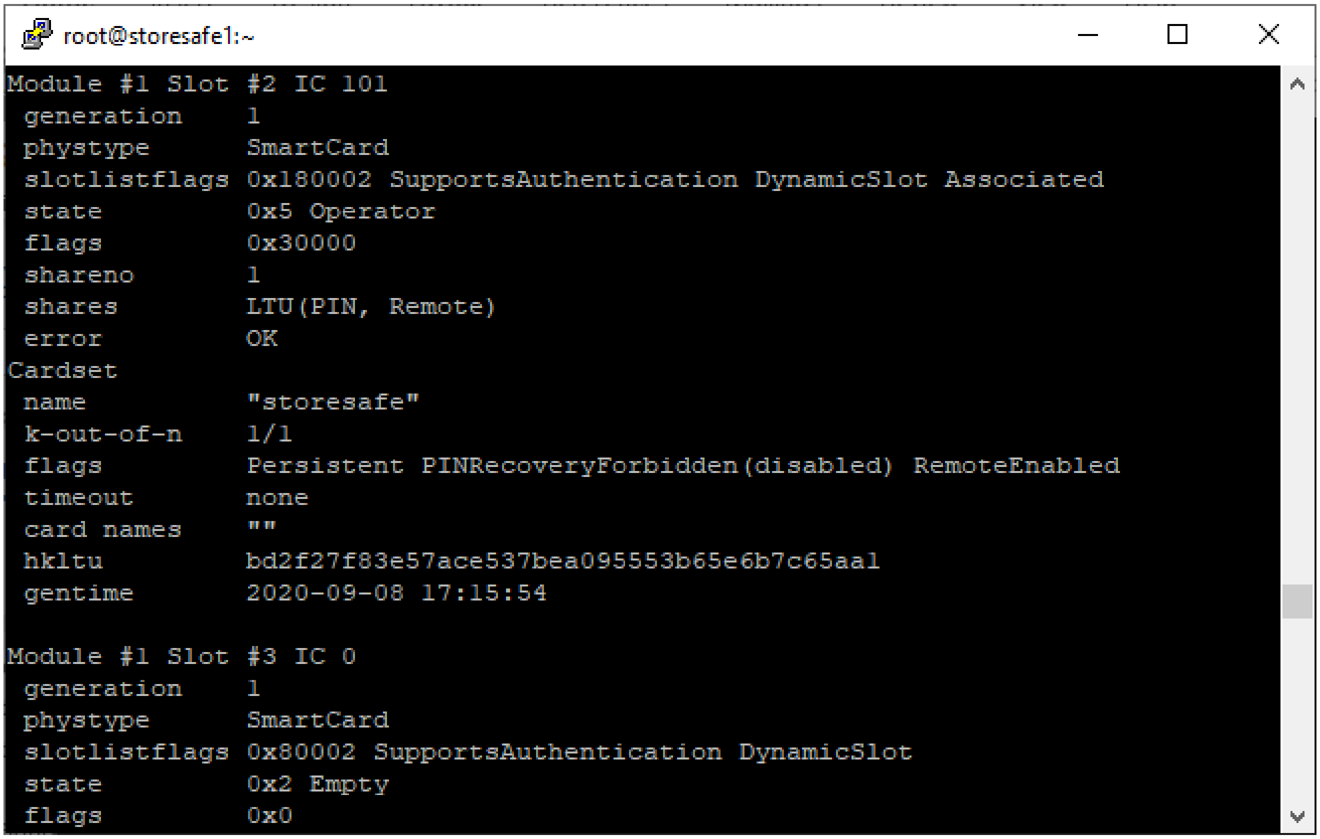
The failback operation of Bloombase StoreSafe High Availability Cluster is fully transparent to users and software applications relying on the data path secured by Bloombase StoreSafe.



My IRS password: iloveyou

nCipher nShield Connect HSM Cluster Failback

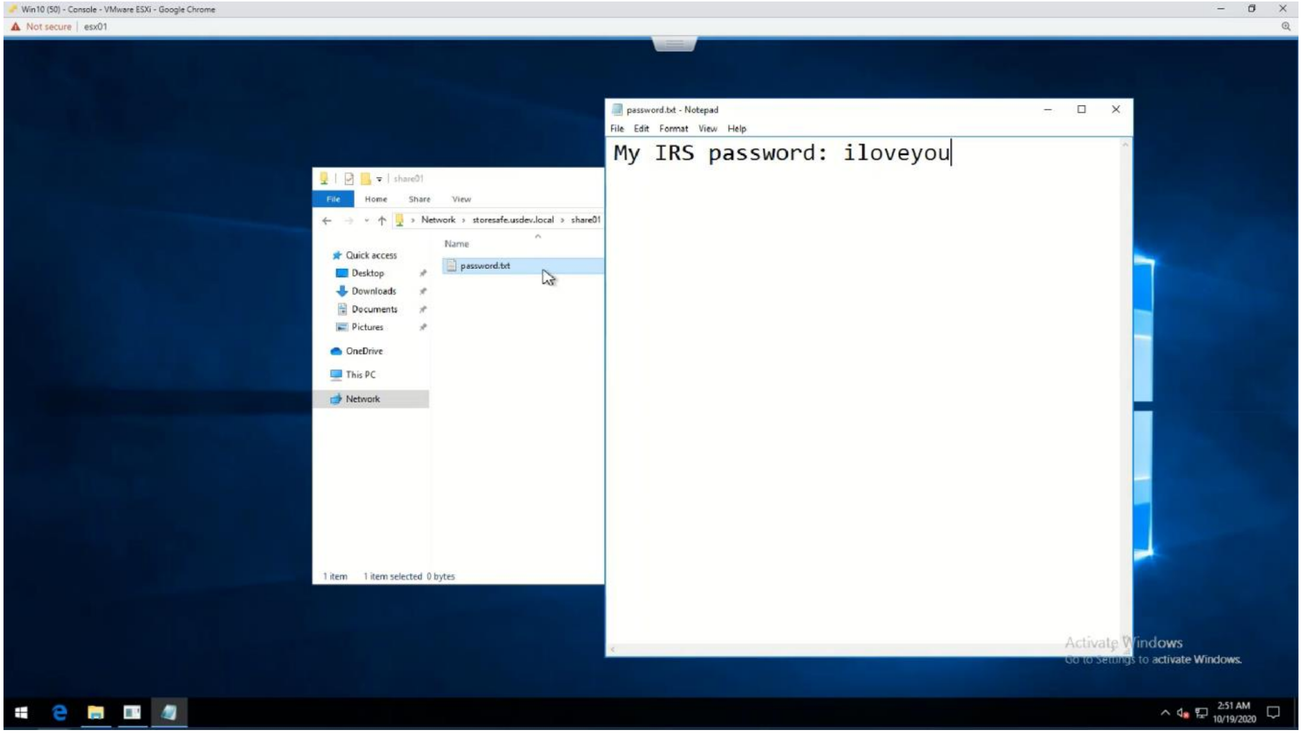
Once any failed nShield HSM module returns to online status, the nfast driver will report the module status again with any active slot statuses.



```
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 .



My IRS password: iloveyou

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	• Microsoft Storage Server • Microsoft Windows Server 2019 • Microsoft Windows 10	• nCipher nShield Connect HSM • nCipher Remote Administration • Trusted Verification Device (TVD) • nCipher Security World

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

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

8. Bloombase is nCipher Security Partner, https://www.ncipher.com/partners/bloombase