interopLab

Bloombase StoreSafe and HashiCorp Vault Integration Guide for Data-at-Rest Encryption

November 2021

BLOOMBASE®

Executive Summary

HashiCorp Vault has been validated by Bloombase InteropLab to run with Bloombase StoreSafe Intelligent Storage Firewall. This document describes the steps carried out to integrate HashiCorp Vault with Bloombase StoreSafe software appliance on VMware ESXi to deliver high bandwidth transparent storage encryption for mission critical applications. Client host system Microsoft Windows 11 has been tested with HashiCorp Vault and Bloombase StoreSafe data-at-rest encryption solution to secure Microsoft Storage Server 2022 storage backend.

Document No.: BLBS-TN - Bloombase StoreSafe HashiCorp Vault Integration Guide - USLET-EN-R0.95

Table of Contents

Purpose and Scope

This document describes the steps necessary to integrate HashiCorp Vault 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 software appliance
- Integrate Bloombase StoreSafe with HashiCorp Vault
- Integrate application components Microsoft Windows 11 client host system and Microsoft Storage Server 2022 with Bloombase StoreSafe and HashiCorp Vault to demonstrate how high-bandwidth, agentless, application-transparent data encryption could be achieved for multiple network storage protocols namely SMB, NFS and iSCSI

Assumptions

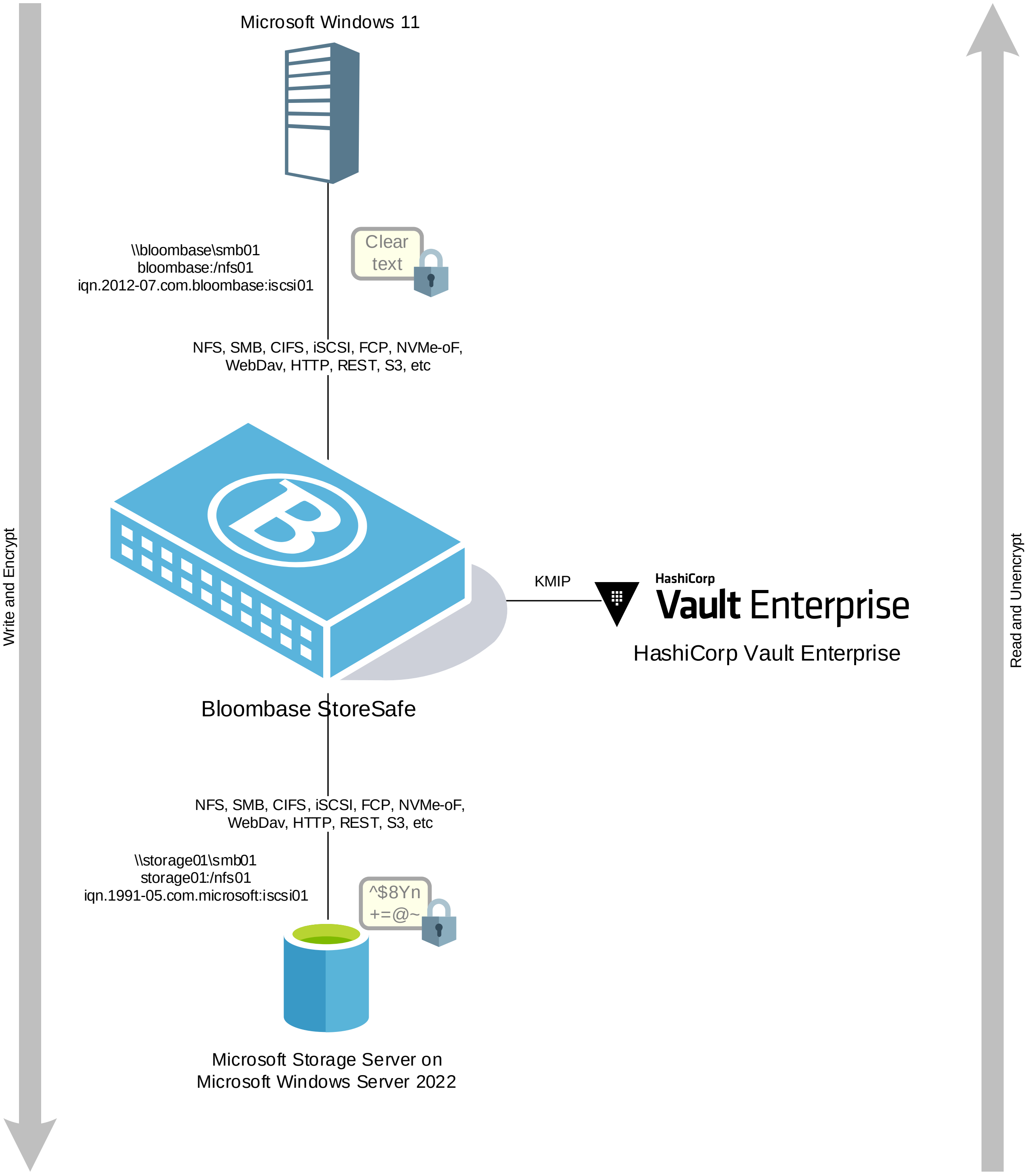
This document describes the integration of HashiCorp Vault with Bloombase StoreSafe. It is assumed that you are familiar with operation of HashiCorp Vault, storage systems, and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is also assumed that you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

As HashiCorp Vault is third party option to Bloombase StoreSafe data at-rest encryption security solution, you are recommended to refer to installation and configuration guides of specific model of HashiCorp Vault 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 and Bloombase SupPortal https://supportal.bloombase.com.

Infrastructure

Setup

The integration discussed in this guide is based on the system block diagram below:


Microsoft Windows 11
\\bloombase\smb01
bloombase:/nfs01
iqn.2012-07.com.bloombase:iscsi01
Clear text
NFS, SMB, CIFS, iSCSI, FCP, NVMe-oF,
WebDav, HTTP, REST, S3, etc
Write and Encrypt
KMIP
HashiCorp
Vault Enterprise
HashiCorp Vault Enterprise
Read and Unencrypt
Bloombase StoreSafe
NFS, SMB, CIFS, iSCSI, FCP, NVMe-oF,
WebDav, HTTP, REST, S3, etc
\\storage01\smb01
storage01:/nfs01
iqn.1991-05.com.microsoft:iscsi01
^$8Yn
+=@~
Microsoft Storage Server on
Microsoft Windows Server 2022

Key Management

Key Manager	HashiCorp Vault 1.8.3+ent

Storage Encryption

Storage Encryption	Bloombase StoreSafe Intelligent Storage Firewall Software Appliance v3.4.8.4-EA2
Server	VMware Virtual Machine (VM) on VMware ESXi 6.5
Processor	4 x Virtual CPU (vCPU)
Memory	8 GB

Storage System

Storage System	Microsoft Storage Server on Microsoft Windows Server 2022 on VMware ESXi 6.5

Application Client

Client Host	Microsoft Windows 11 on VMware ESXi 6.5

Configuration Overview

HashiCorp Vault

HashiCorp Vault is an identity-based secrets and encryption management system. Vault provides encryption services that are gated by authentication and authorization methods. Arbitrary key/value secrets can be stored in Vault. Vault encrypts these secrets prior to writing them to persistent storage, so gaining access to the raw storage isn't enough to access your secrets.

The HashiCorp Vault provides central management and secure storage of encryption keys, including those generated by Bloombase StoreSafe products, and KMIP-compliant cloud vendors. It provides intuitive web-based console, and APIs for managing of encryption keys.

The KMIP services provided by HashiCorp Vault are used by Bloombase StoreSafe for encryption protection of data-at-rest use cases.

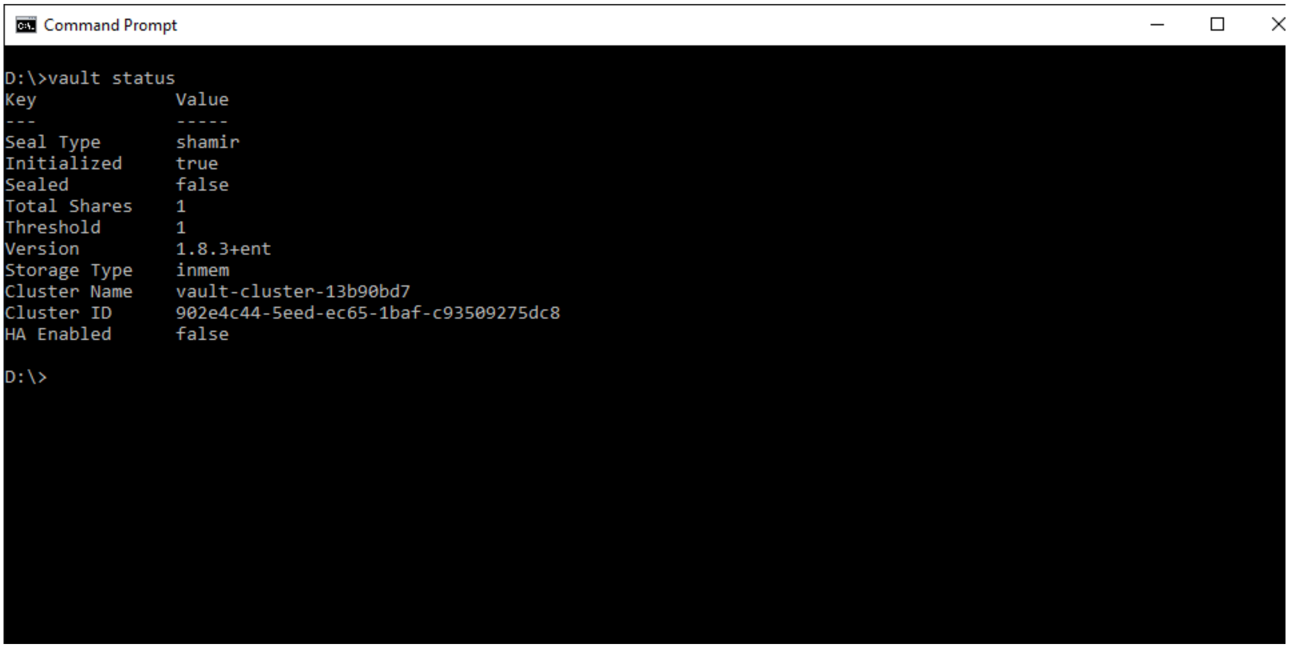
HashiCorp Vault Configurations

Assume HashiCorp Vault is installed and configured as a network attached appliance with IP address

```
192.168.23.131
```

HashiCorp Vault can be managed remotely via CLI-based text console at address:

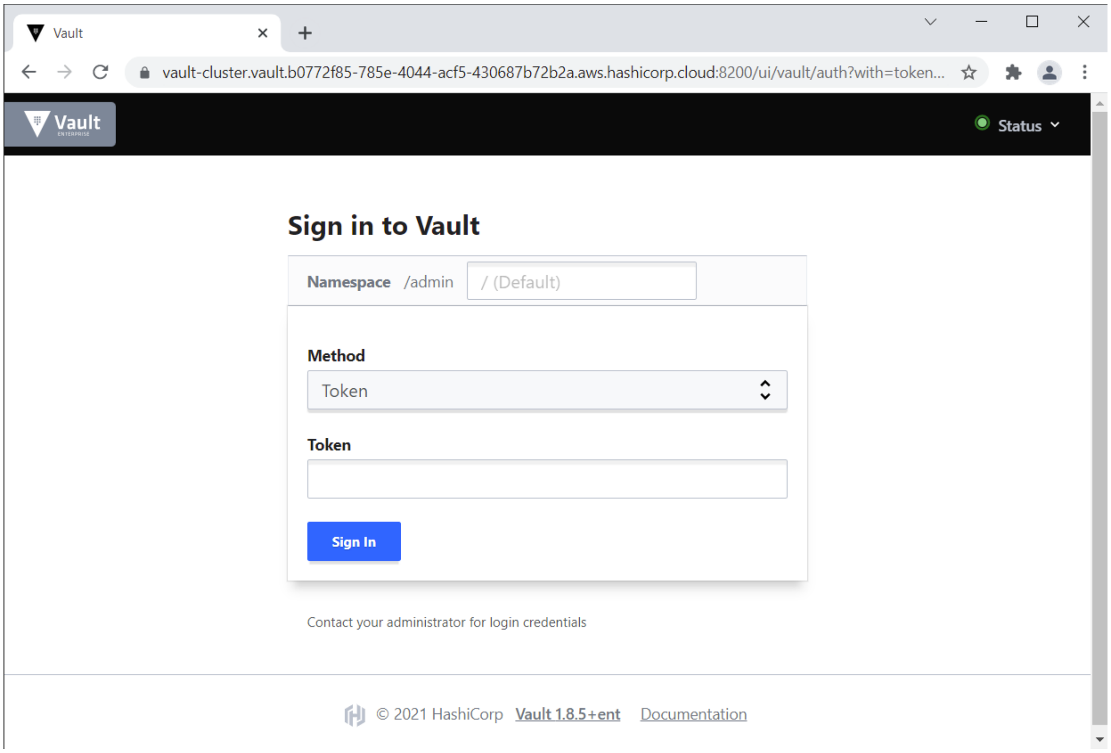
```
https:// 192.168.23.131:8200
```



```
D:\>vault status
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    1
Threshold       1
Version         1.8.3+ent
Storage Type    inmem
Cluster Name    vault-cluster-13b90bd7
Cluster ID      902e4c44-5eed-ec65-1baf-c93509275dc8
HA Enabled      false

D:\>
```

Alternatively, the web dashboard of the HashiCorp Vault can be accessed at the same address:

```
https:// 192.168.23.131:8200
```



vault-cluster.vault.b0772f85-785e-4044-acf5-430687b72b2a.aws.hashicorp.cloud:8200/ui/vault/auth?with=token...

Sign in to Vault

Namespace /admin / (Default)

Method: Token

Token:

Contact your administrator for login credentials

© 2021 HashiCorp Vault 1.8.5+ent Documentation

HashiCorp Vault Client Enrollment

To establish the trust and allow communication between HashiCorp Vault and Bloombase StoreSafe, certificates need to be created and stored in the HashiCorp Vault and the Bloombase StoreSafe. In the HashiCorp Vault, this can be configured as follows.

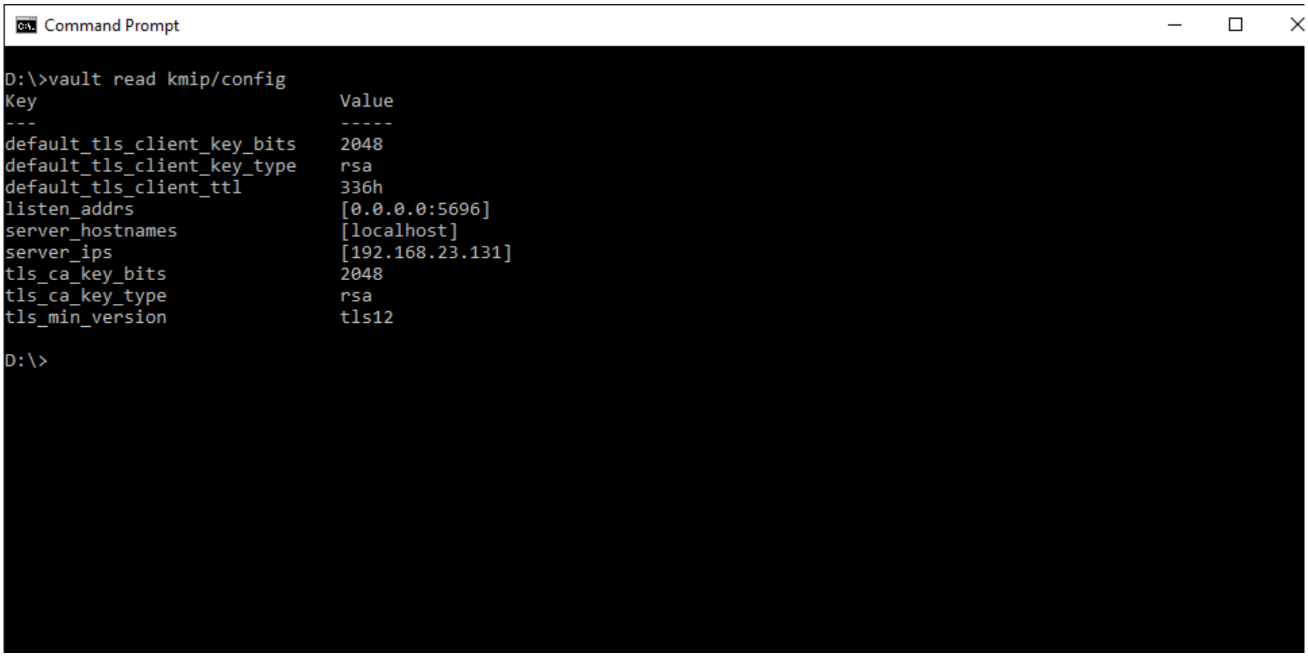
Enable the KMIP feature, with the network address, and other configurations. For example:

```
vault secrets enable kmip
vault write kmip/config listen_addrs=0.0.0.0:5696 \
     server_ips="192.168.23.131" \
     tls_ca_key_type="rsa" \
     tls_ca_key_bits=2048 \
     default_tls_client_key_type="rsa" \
     default_tls_client_key_bits=2048
```

Create a scope and role:

```
vault write -f kmip/scope/bloombase
vault write kmip/scope/bloombase/role/admin operation_all=true
```

An example configuration can be seen in the figure below:



```
D:\>vault read kmip/config
Key                            Value
---                            -----
default_tls_client_key_bits    2048
default_tls_client_key_type    rsa
default_tls_client_ttl         336h
listen_addrs                   [0.0.0.0:5696]
server_hostnames               [localhost]
server_ips                     [192.168.23.131]
tls_ca_key_bits                2048
tls_ca_key_type                rsa
tls_min_version                tls12

D:\>
```

KMIP client certificate and key is generated and downloaded from HashiCorp Vault. Download the Certificate and upload to the Bloombase StoreSafe trusted client configuration.

Note, you are **required** to convert the JSON format (key and certificate) to PKCS #12 format in order to upload to the Bloombase StoreSafe.

```
vault write -format=json kmip/scope/bloombase/role/admin/credential/generate format=pem >
vault_credential.json
```

Also, download the HashiCorp Vault CA certificate which will be needed to be imported to the trusted server configuration at the Bloombase StoreSafe

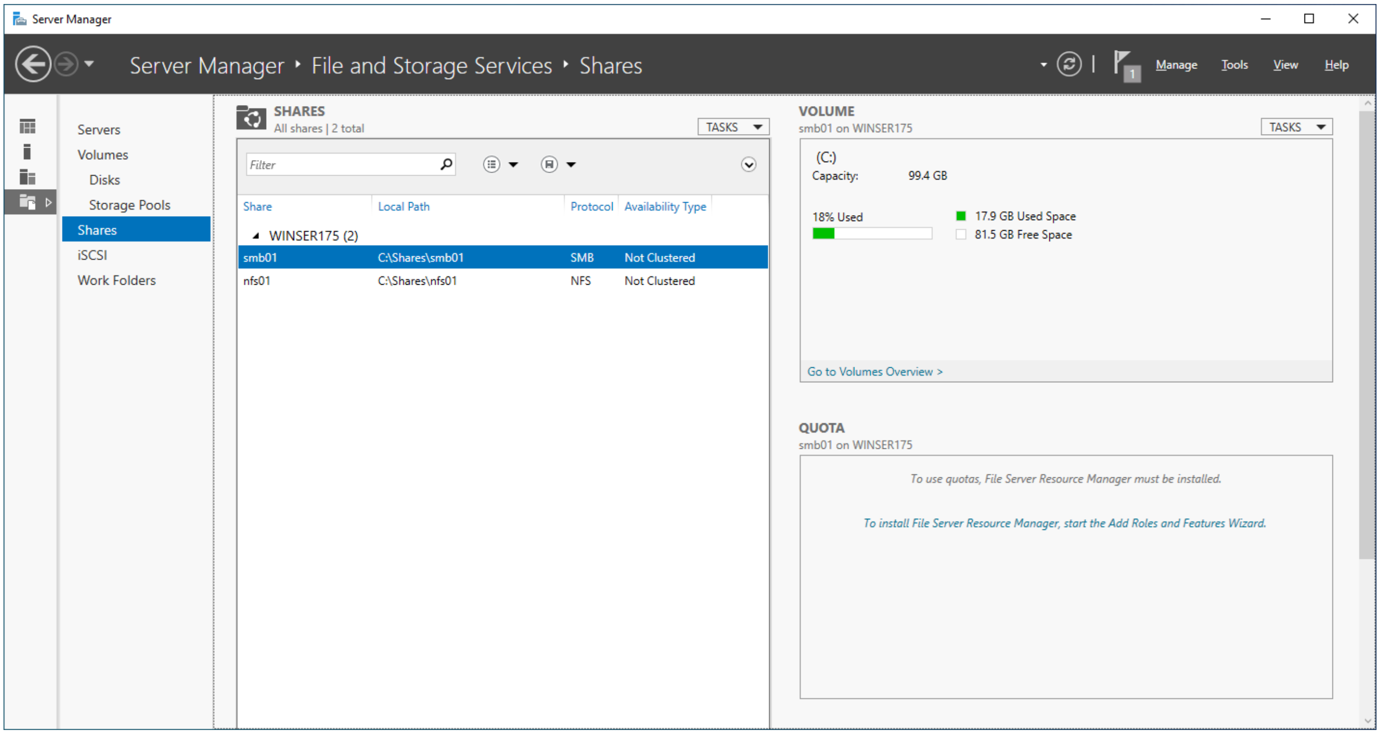
```
vault read kmip/ca
```

Microsoft Storage Server on Microsoft Windows Server 2022

Microsoft Storage Server on Microsoft Windows Server 2022 running on VMware ESXi is used in this interoperability test which is able to provide storage services over network storage protocols including NVMe-oF, FCP, iSCSI, NFS, SMB, CIFS, REST, etc.

Microsoft Windows Server 2022 is deployed as a virtual machine (VM) on VMware ESXi.

SMB Services Configuration



SHARES
All shares | 2 total

Share	Local Path	Protocol	Availability Type
◢ WINSER175 (2)			
smb01	C:\Shares\smb01	SMB	Not Clustered
nfs01	C:\Shares\nfs01	NFS	Not Clustered

VOLUME
smb01 on WINSER175

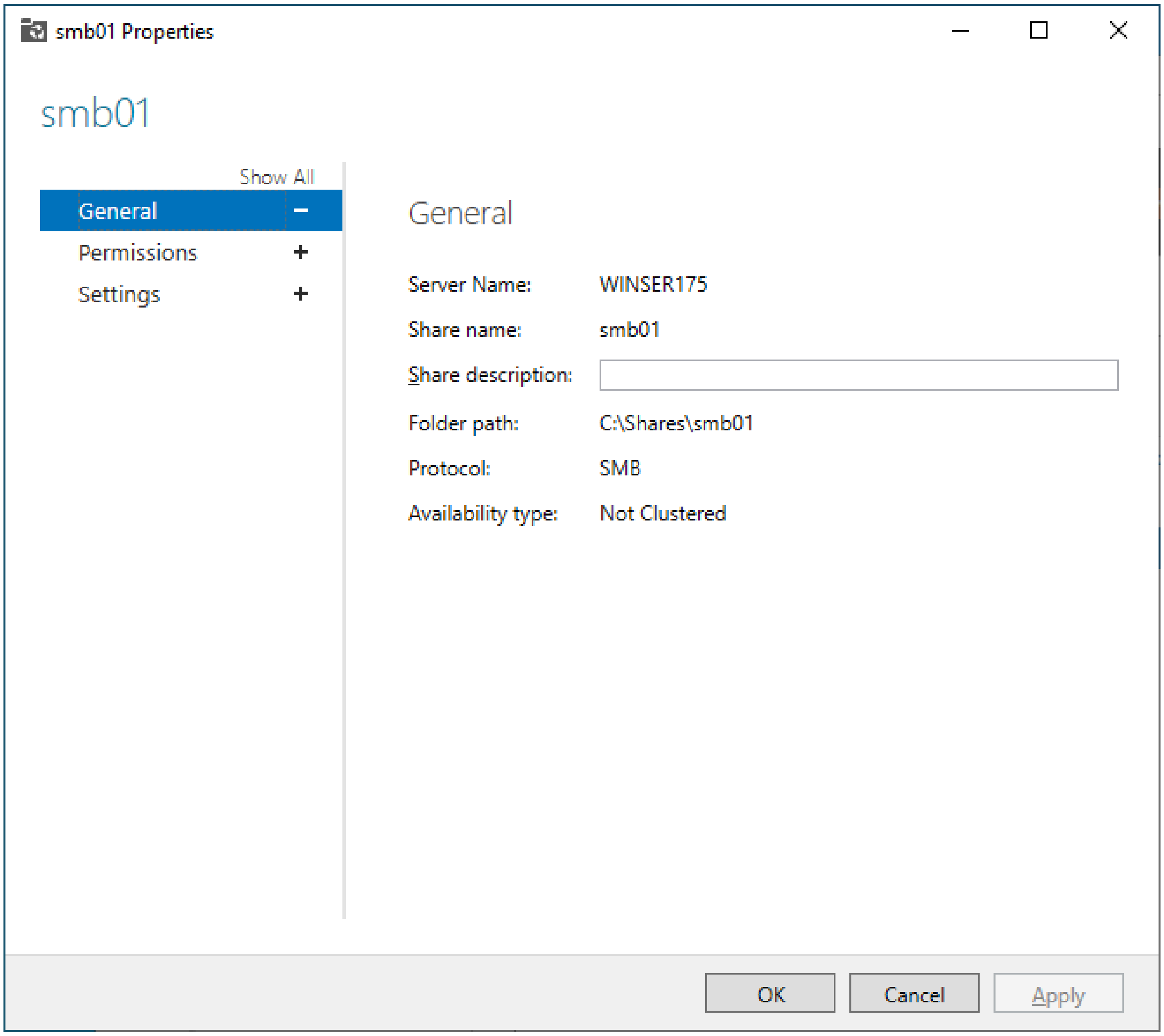
(C:)
Capacity: 99.4 GB

18% Used
🟩 17.9 GB Used Space
□ 81.5 GB Free Space

QUOTA
smb01 on WINSER175

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

To install File Server Resource Manager, start the Add Roles and Features Wizard.



Server Name: WINSER175

Share name: smb01

Share description:

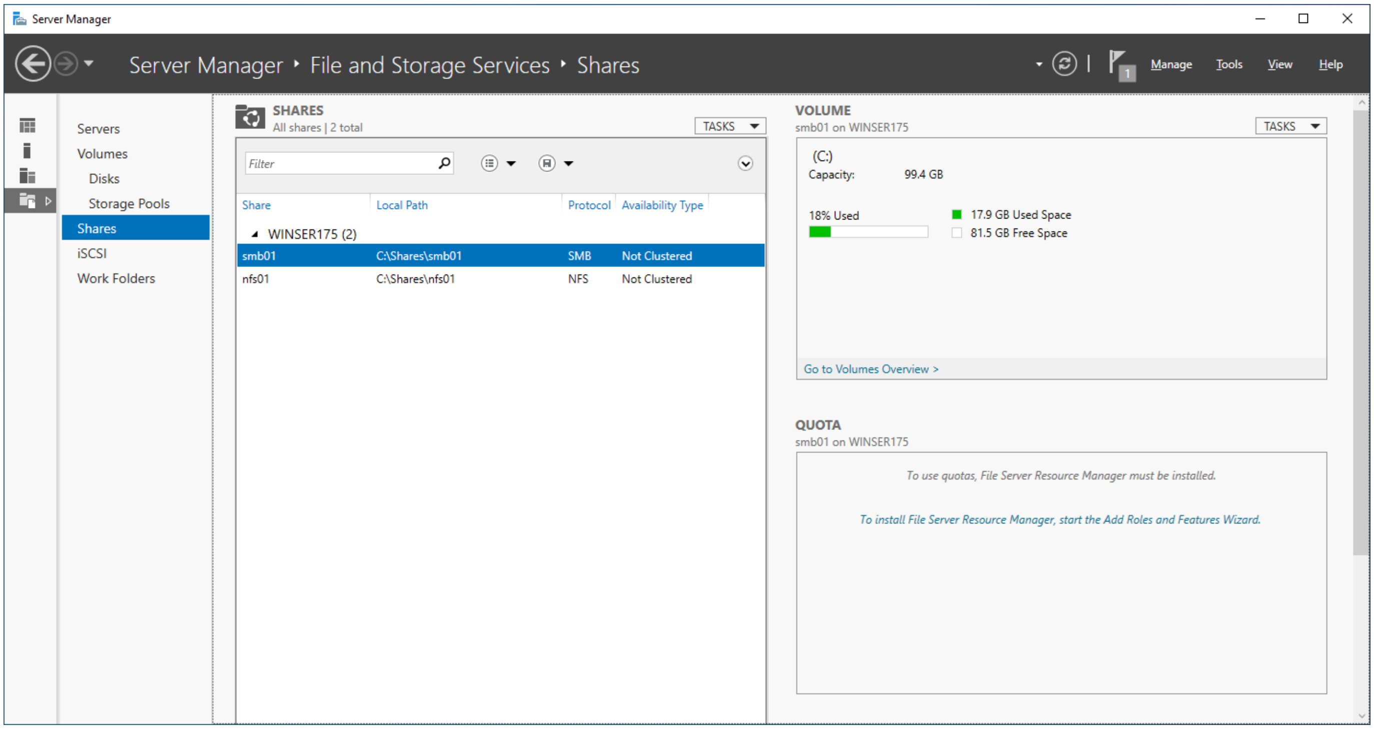
Folder path: C:\Shares\smb01

Protocol: SMB

Availability type: Not Clustered

Microsoft Windows Server 2022 File Management is configured to provide the SMB share backend storage to client system users.

NFS Services Configuration



SHARES
All shares | 2 total

Share	Local Path	Protocol	Availability Type
◢ WINSER175 (2)			
smb01	C:\Shares\smb01	SMB	Not Clustered
nfs01	C:\Shares\nfs01	NFS	Not Clustered

VOLUME
smb01 on WINSER175

(C:)
Capacity: 99.4 GB

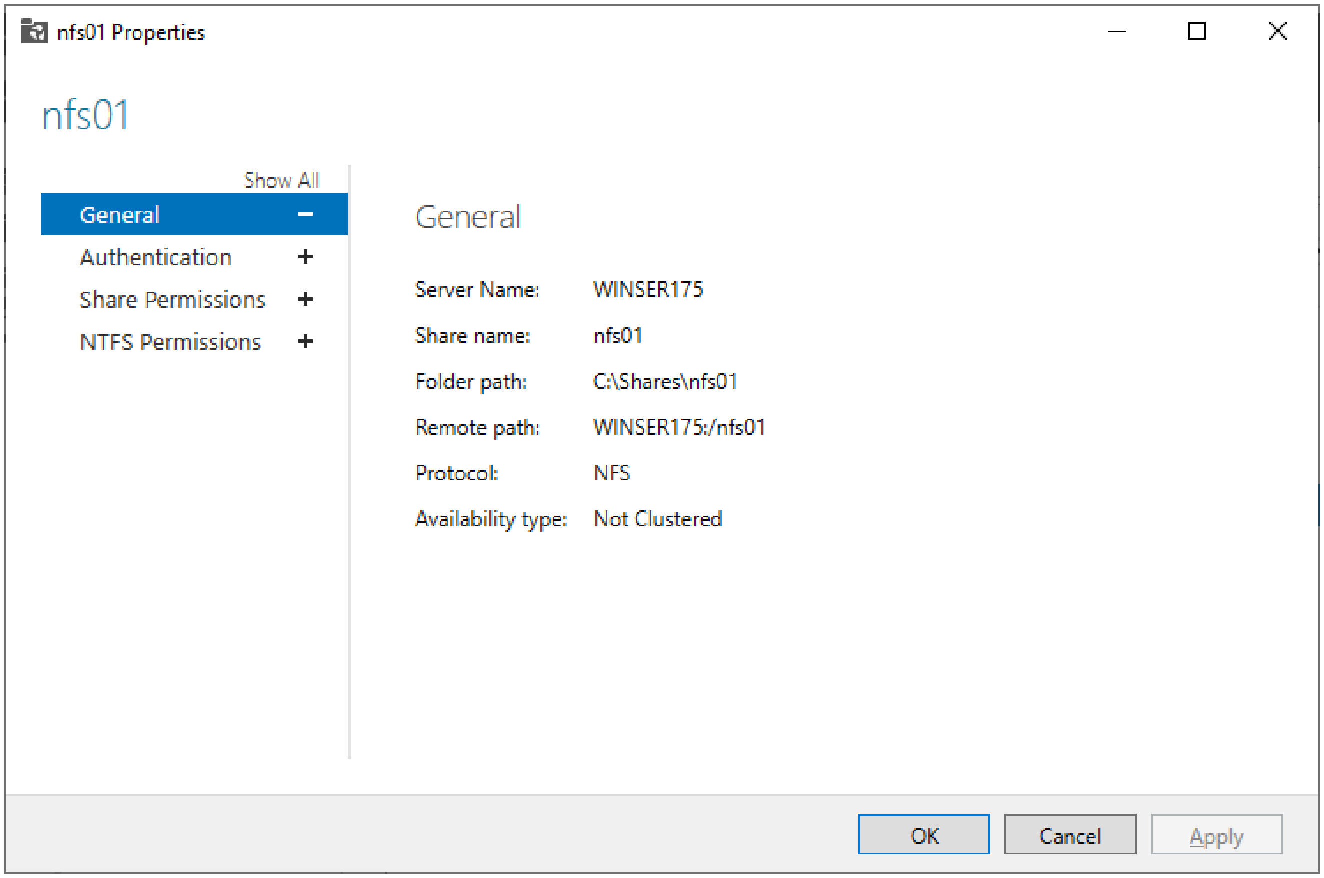
18% Used
🟩 17.9 GB Used Space
□ 81.5 GB Free Space

Go to Volumes Overview >

QUOTA
smb01 on WINSER175

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

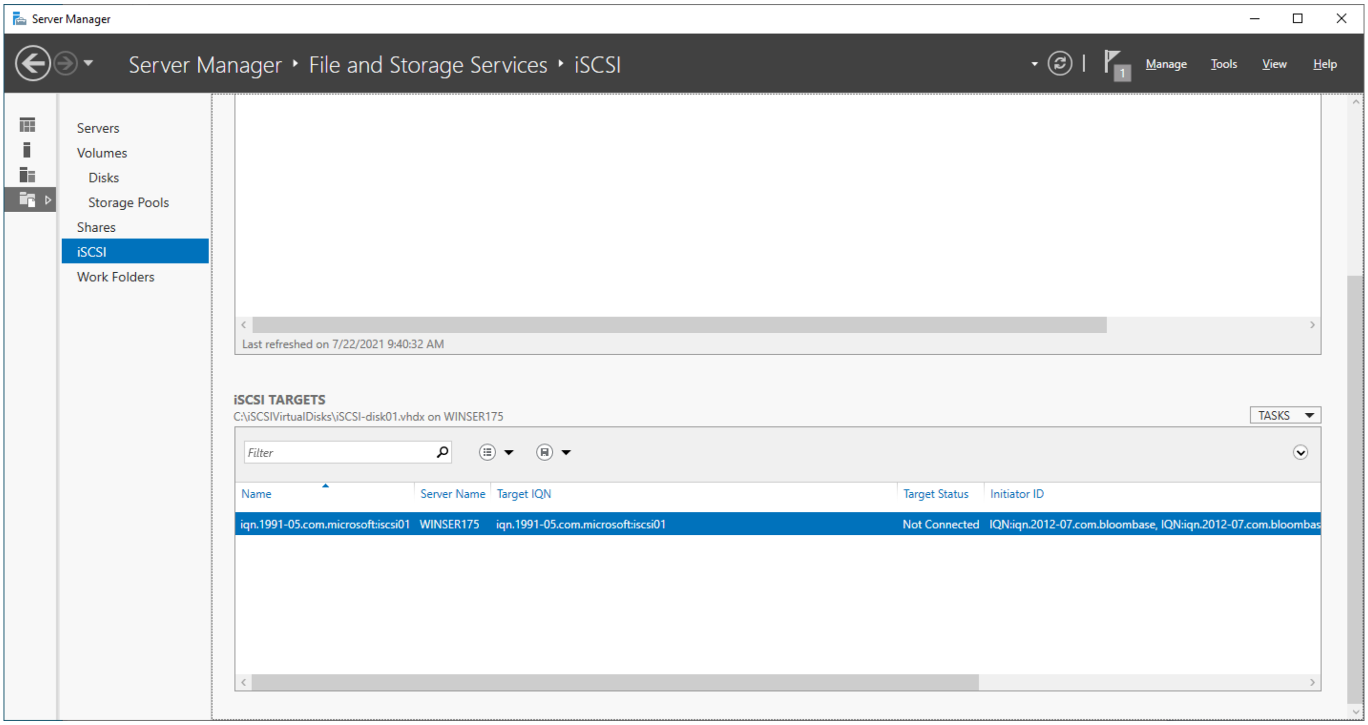
To install File Server Resource Manager, start the Add Roles and Features Wizard.



Server Name: WINSER175
Share name: nfs01
Folder path: C:\Shares\nfs01
Remote path: WINSER175:/nfs01
Protocol: NFS
Availability type: Not Clustered

NFS storage service is provisioned on Microsoft Windows Server 2022 to be used in this integration testing.

iSCSI Services Configuration



Last refreshed on 7/22/2021 9:40:32 AM

iSCSI TARGETS

C:\iSCSIVirtualDisks\iSCSI-disk01.vhdx on WINSER175

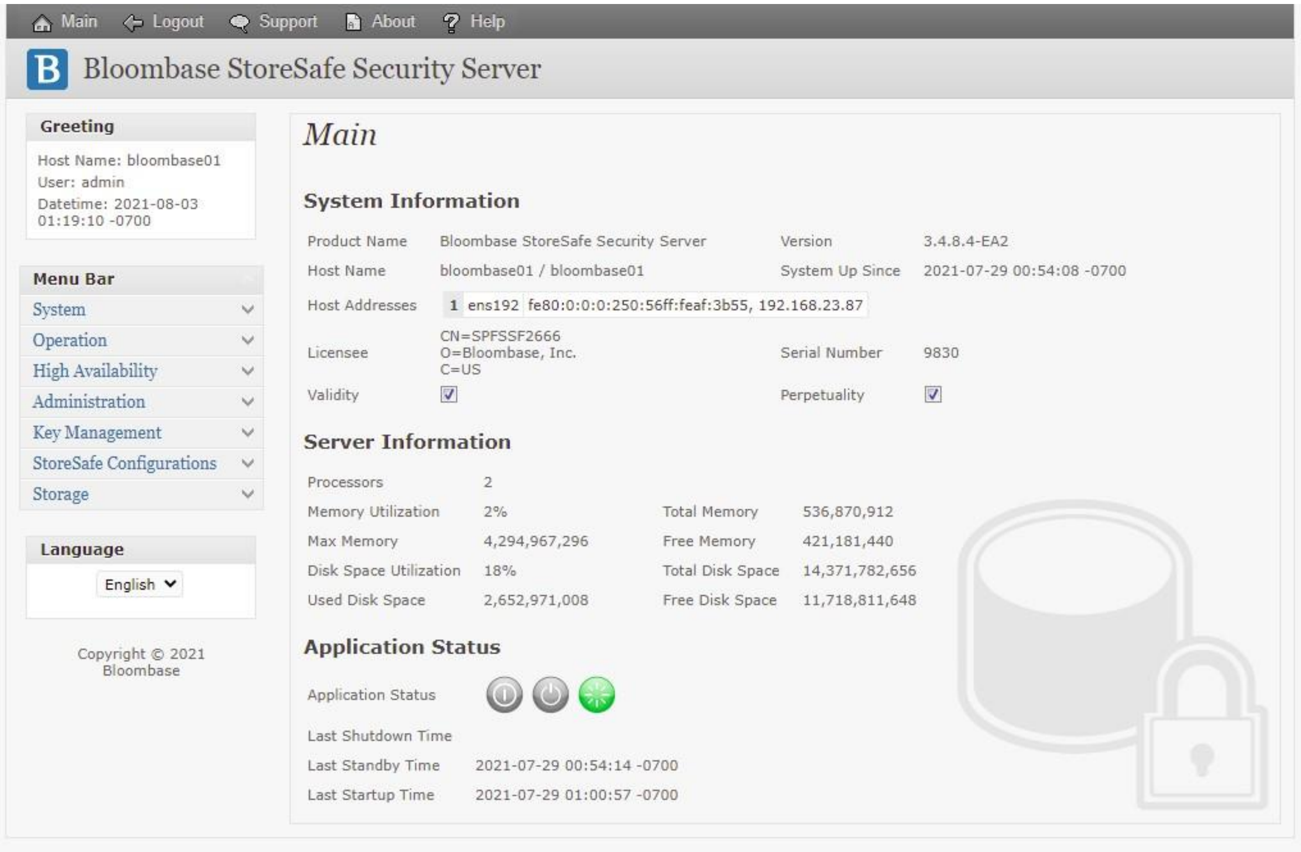
Name	Server Name	Target IQN	Target Status	Initiator ID
iqn.1991-05.com.microsoft:iscsi01	WINSER175	iqn.1991-05.com.microsoft:iscsi01	Not Connected	IQN:iqn.2012-07.com.bloombase, IQN:iqn.2012-07.com.bloombas

iSCSI storage service is also provisioned on Microsoft Windows Server 2022 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, both file-based and block-based encryption security services are validated against Bloombase StoreSafe with keys managed at HashiCorp Vault.

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



Host Name: bloombase01
User: admin
Datetime: 2021-08-03 01:19:10 -0700

Main

System Information

Product Name	Bloombase StoreSafe Security Server	Version	3.4.8.4-EA2
Host Name	bloombase01 / bloombase01	System Up Since	2021-07-29 00:54:08 -0700
Host Addresses	1 ens192 fe80:0:0:0:250:56ff:feaf:3b55, 192.168.23.87		

Licensee	CN=SPFSSF2666
	O=Bloombase, Inc.
	C=US
		Serial Number	9830

Validity	☑	Perpetuality	☑

Server Information

Processors	2		
Memory Utilization	2%	Total Memory	536,870,912
Max Memory	4,294,967,296	Free Memory	421,181,440
Disk Space Utilization	18%	Total Disk Space	14,371,782,656
Used Disk Space	2,652,971,008	Free Disk Space	11,718,811,648

Application Status

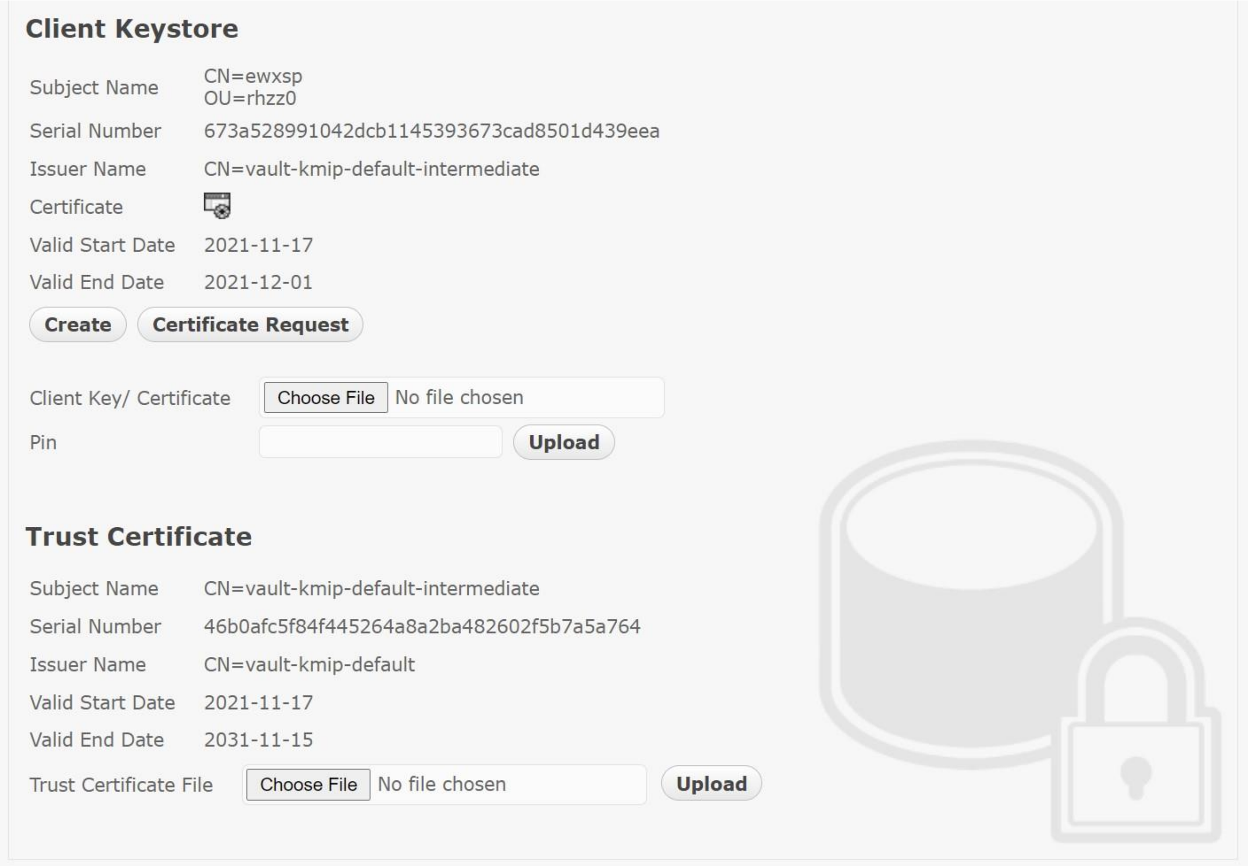
Application Status	
Last Shutdown Time	
Last Standby Time	2021-07-29 00:54:14 -0700
Last Startup Time	2021-07-29 01:00:57 -0700

HashiCorp Vault and Bloombase StoreSafe Integration

Bloombase StoreSafe Intelligent Storage Firewall supports HashiCorp Vault out of the box due to the fact that both products support OASIS Key Management Interoperability Protocol (KMIP).

To enable the built-in Bloombase KeyCastle to utilize keys managed in the network attached HashiCorp Vault, the KMIP service configuration at Bloombase web management console has to be set up.

First of all, import HashiCorp Vault’s X.509 client key pair as “Client Keystore” and server certificate into “Trust Certificate” at the Bloombase StoreSafe web management console so as to establish the trust between Bloombase StoreSafe and HashiCorp Vault.



Client Keystore

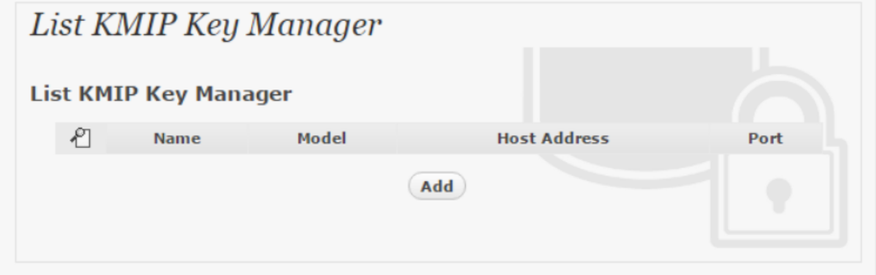
Subject Name	CN=ewxsp
	OU=rhzz0

Serial Number	673a528991042dcb1145393673cad8501d439eea
Issuer Name	CN=vault-kmip-default-intermediate
Certificate	
Valid Start Date	2021-11-17
Valid End Date	2021-12-01

Trust Certificate

Subject Name	CN=vault-kmip-default-intermediate
Serial Number	46b0afc5f84f445264a8a2ba482602f5b7a5a764
Issuer Name	CN=vault-kmip-default
Valid Start Date	2021-11-17
Valid End Date	2031-11-15

Next, add the HashiCorp Vault instance to the Bloombase StoreSafe KMIP configuration. This is done by clicking “OASIS KMIP Key Manager” under “Key Management”.



List KMIP Key Manager

List KMIP Key Manager

	Name	Model	Host Address	Port

Input a name for the HashiCorp Vault

```
vault01
```

and select Model as

```
HashiCorp Vault
```

Input also the host name

```
vault01
```

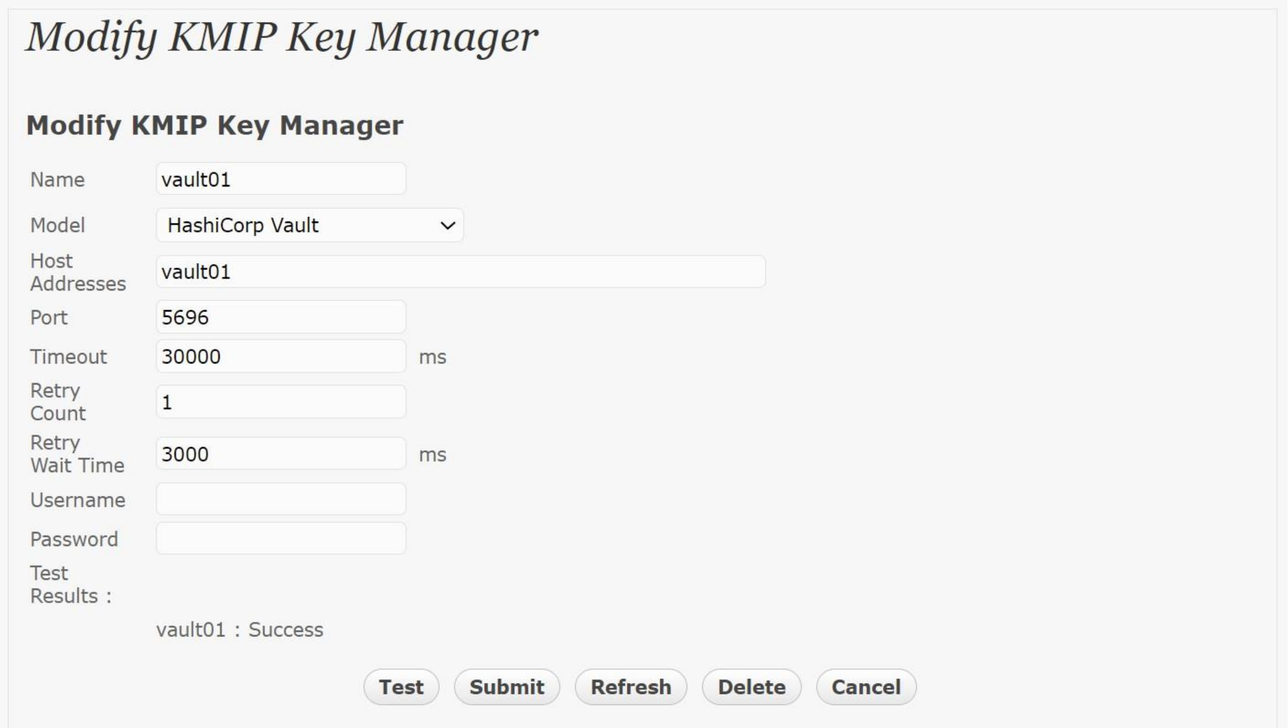
or IP address

```
192.168.23.131
```

and KMIP service port

```
5696
```

to access the HashiCorp Vault.



Modify KMIP Key Manager

Modify KMIP Key Manager

Name	vault01
Model	HashiCorp Vault
Host Addresses	vault01
Port	5696
Timeout	30000 ms
Retry Count	1
Retry Wait Time	3000 ms
Username	
Password	
Test Results :	
	vault01 : Success

Click 'Submit' to commit the configuration. If the certificates are setup properly, "Test Results" of the KMIP Key Manager would return "Success".

Encryption Key Provisioning

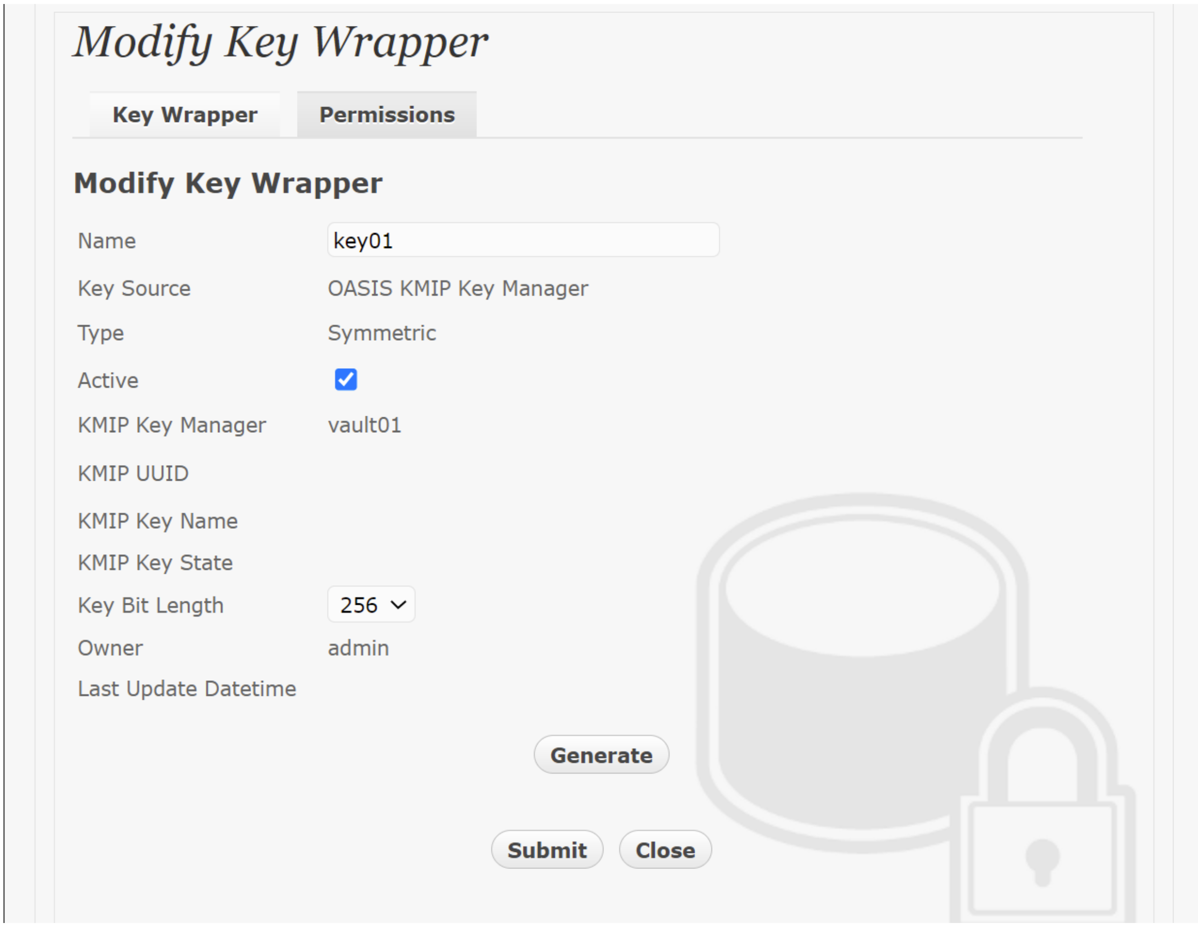
To generate key in attached HashiCorp Vault, select Key Source Type as

```
OASIS KMIP Key Manager
```

and the assigned Key Manager label, in this case

```
vault01
```

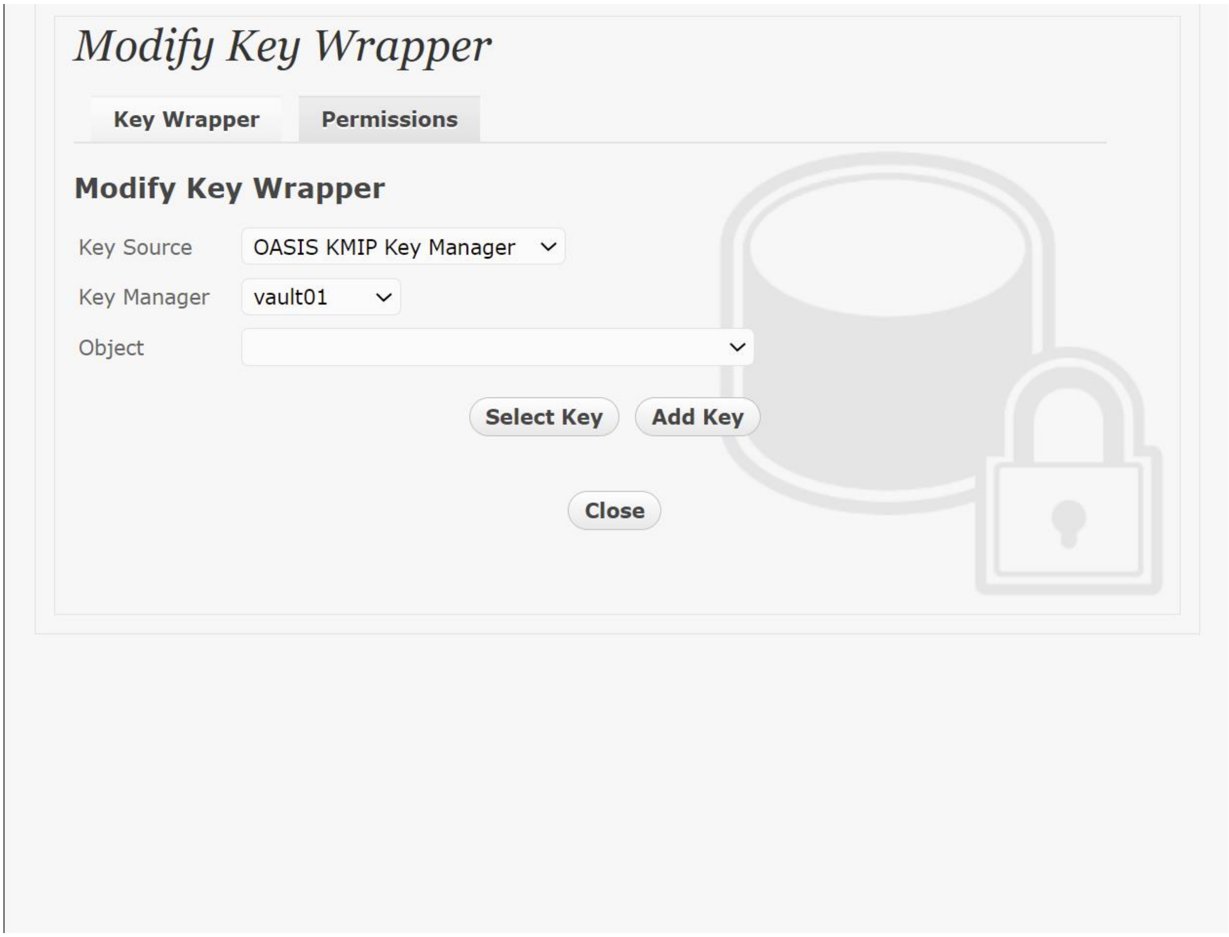
Select "Add Key" and "generate" to create a new key on the HSM.



Modify Key Wrapper

Name	key01
Key Source	OASIS KMIP Key Manager
Type	Symmetric
Active	☑
KMIP Key Manager	vault01
KMIP UUID	
KMIP Key Name	
KMIP Key State	
Key Bit Length	256
Owner	admin
Last Update Datetime	

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

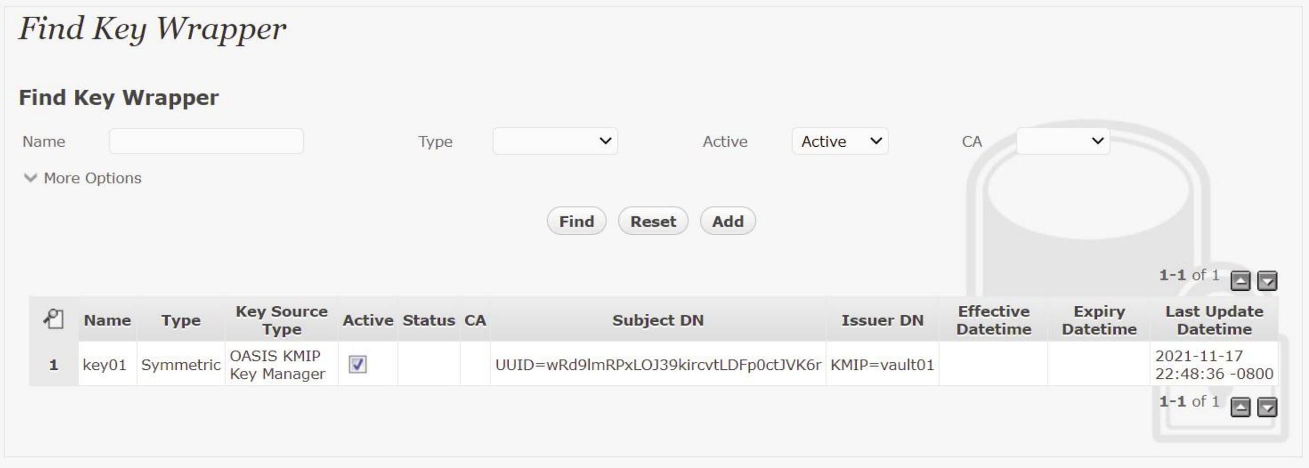


Modify Key Wrapper

Modify Key Wrapper

Key Source	OASIS KMIP Key Manager
Key Manager	vault01
Object	

Ensure that you import a key from the KMIP key manager before you submit the key wrapper at Bloombase StoreSafe.



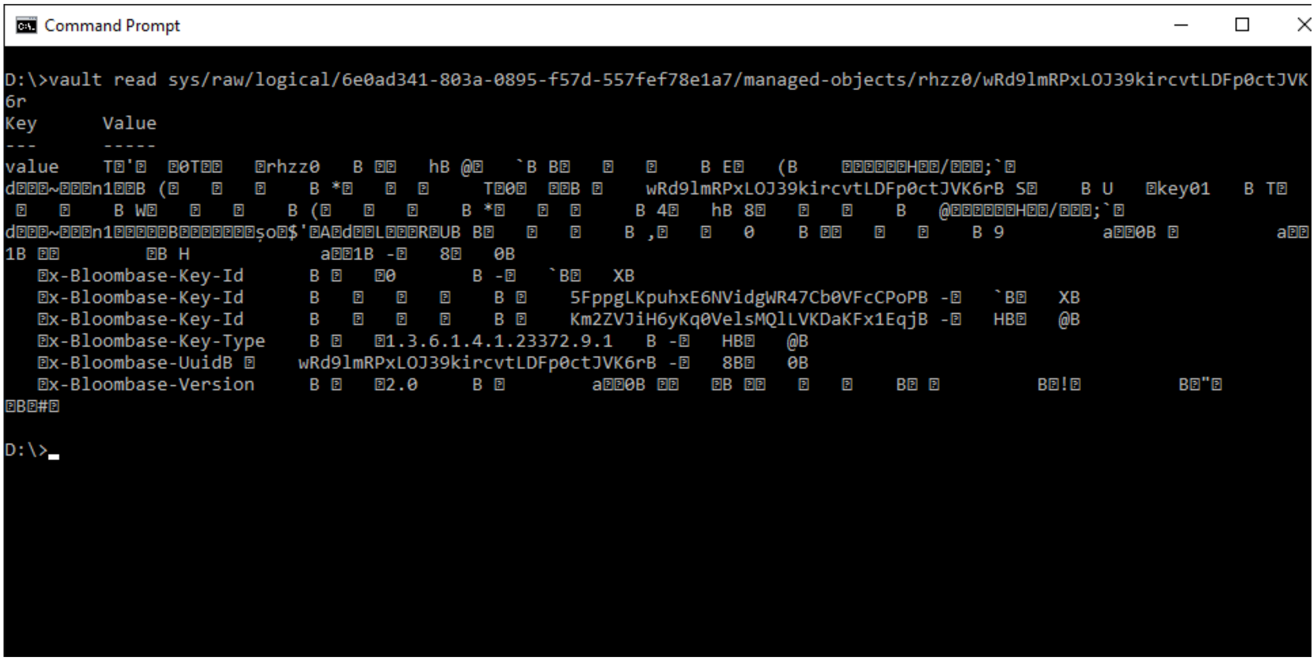
Find Key Wrapper

Find Key Wrapper

Name		Type		Active	Active	CA	

	Name	Type	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1	key01	Symmetric	OASIS KMIP Key Manager	☑			UUID=wRd9lmRPxLOJ39kircvtLDFp0ctJVK6r	KMIP=vault01			2021-11-17 22:48:36 -0800

Cross check at the HashiCorp Vault console that the newly generated key can be found on the HashiCorp Vault server.



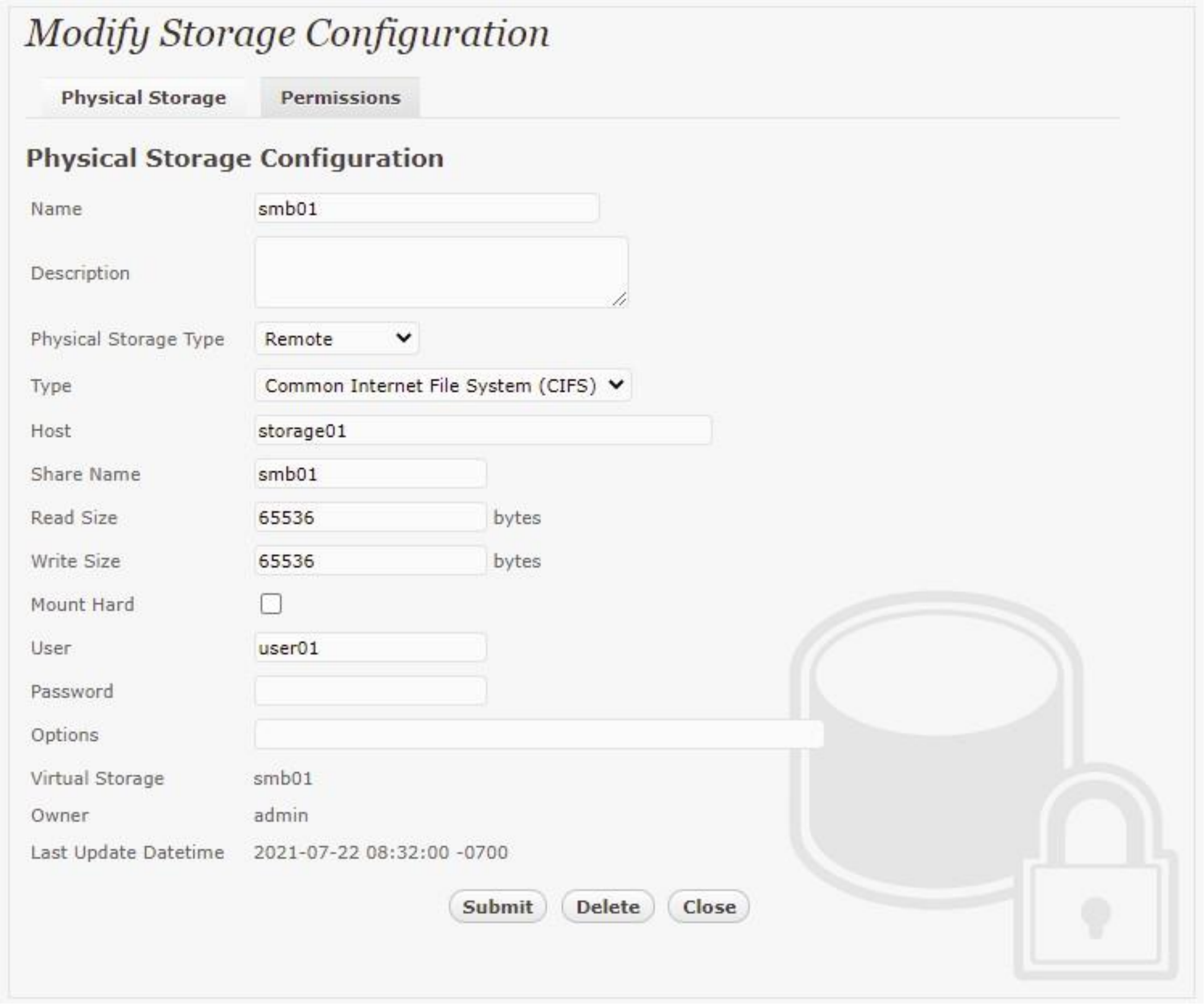
```
D:\>vault read sys/raw/logical/6e0ad341-803a-0895-f57d-557fef78e1a7/managed-objects/rhzz0/wRd9lmRPxLOJ39kircvtLDFp0ctJVK
6r
Key      Value
---      -----
value    T⍰'⍰  ⍰0T⍰⍰   ⍰rhzz0   B ⍰⍰   hB @⍰   `B B⍰   ⍰   ⍰    B E⍰   (B    ⍰⍰⍰⍰⍰⍰H⍰⍰/⍰⍰⍰;`⍰
d⍰⍰⍰~⍰⍰⍰n1⍰⍰B (⍰   ⍰   ⍰    B *⍰   ⍰  ⍰     T⍰0⍰  ⍰⍰B ⍰    wRd9lmRPxLOJ39kircvtLDFp0ctJVK6rB S⍰    B U   ⍰key01   B T⍰
 ⍰   ⍰    B W⍰   ⍰   ⍰    B (⍰   ⍰   ⍰    B *⍰   ⍰  ⍰     B 4⍰   hB 8⍰   ⍰   ⍰    B   @⍰⍰⍰⍰⍰⍰H⍰⍰/⍰⍰⍰;`⍰
d⍰⍰⍰~⍰⍰⍰n1⍰⍰⍰⍰⍰B⍰⍰⍰⍰⍰⍰⍰⍰şo⍰$'⍰A⍰d⍰⍰L⍰⍰⍰R⍰UB B⍰   ⍰   ⍰    B ,⍰   ⍰   0    B ⍰⍰   ⍰   ⍰    B 9         a⍰⍰0B ⍰        a⍰⍰
1B ⍰⍰        ⍰B H            a⍰⍰1B -⍰   8⍰   0B
   ⍰x-Bloombase-Key-Id      B ⍰   ⍰0       B -⍰   `B⍰   XB
   ⍰x-Bloombase-Key-Id      B   ⍰   ⍰   ⍰    B ⍰    5FppgLKpuhxE6NVidgWR47Cb0VFcCPoPB -⍰   `B⍰   XB
   ⍰x-Bloombase-Key-Id      B   ⍰   ⍰   ⍰    B ⍰    Km2ZVJiH6yKq0VelsMQlLVKDaKFx1EqjB -⍰   HB⍰   @B
   ⍰x-Bloombase-Key-Type    B ⍰   ⍰1.3.6.1.4.1.23372.9.1   B -⍰   HB⍰   @B
   ⍰x-Bloombase-UuidB ⍰    wRd9lmRPxLOJ39kircvtLDFp0ctJVK6rB -⍰   8B⍰   0B
   ⍰x-Bloombase-Version     B ⍰   ⍰2.0     B ⍰        a⍰⍰0B ⍰⍰   ⍰B ⍰⍰   ⍰   ⍰    B⍰ ⍰         B⍰!⍰         B⍰"⍰
⍰B⍰#⍰

D:\>
```

Data-at-Rest Encryption for SMB

Physical storage namely

```
smb01
```

is configured to be secured by Bloombase StoreSafe using encryption.



Modify Storage Configuration

Physical Storage Configuration

Name	smb01
Description	
Physical Storage Type	Remote
Type	Common Internet File System (CIFS)
Host	storage01
Share Name	smb01
Read Size	65536 bytes
Write Size	65536 bytes
Mount Hard	□
User	user01
Password	
Options	
Virtual Storage	smb01
Owner	admin
Last Update Datetime	2021-07-22 08:32:00 -0700

Virtual storage namely

```
smb01
```

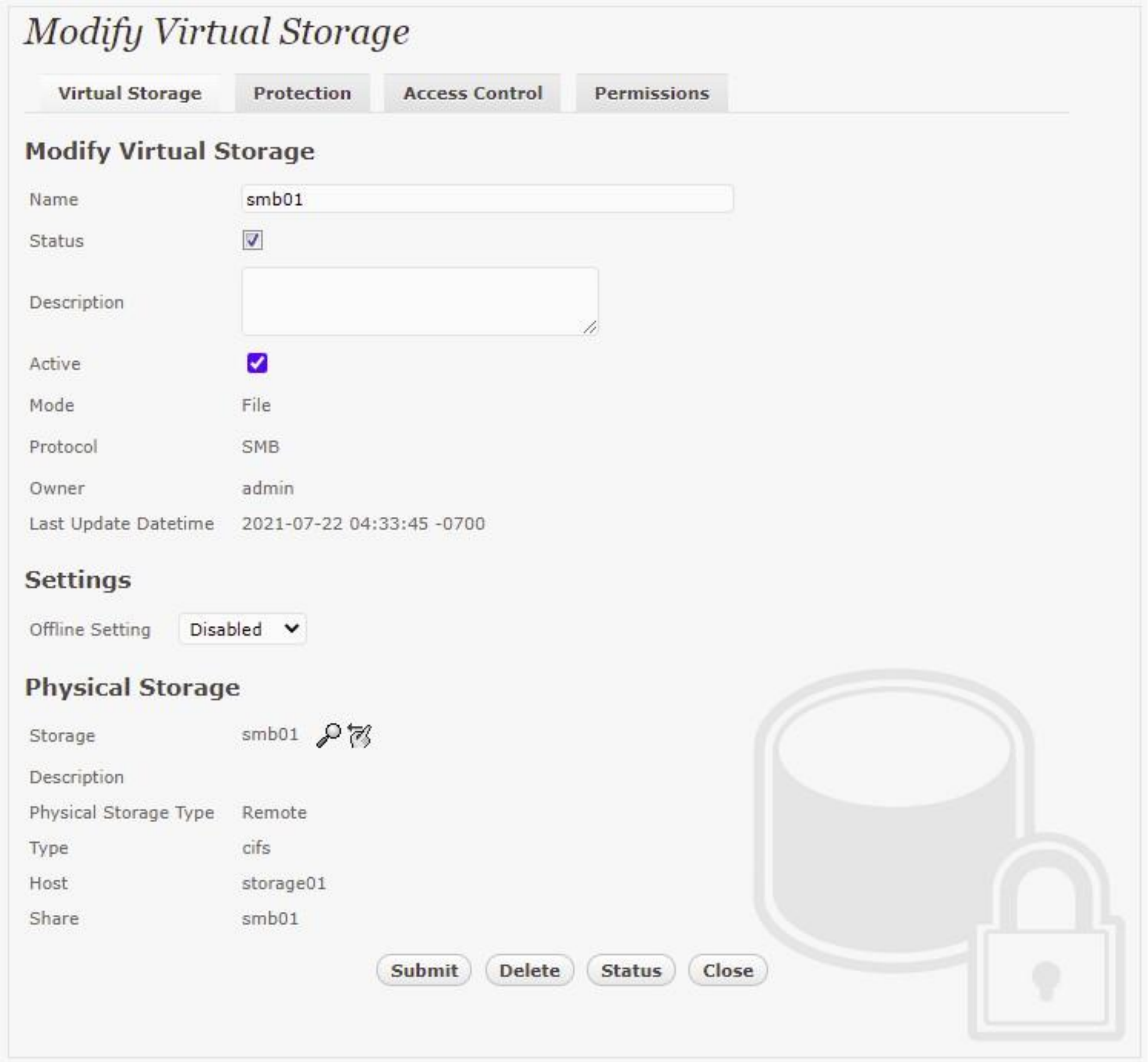
of type

```
File
```

is created to virtualize physical storage

```
smb01
```

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



Modify Virtual Storage

Name	smb01
Status	☑
Description	
Active	☑
Mode	File
Protocol	SMB
Owner	admin
Last Update Datetime	2021-07-22 04:33:45 -0700

Settings

Offline Setting: Disabled

Physical Storage

Storage	smb01
Description	
Physical Storage Type	Remote
Type	cifs
Host	storage01
Share	smb01

Protection type is specified as

```
Privacy
```

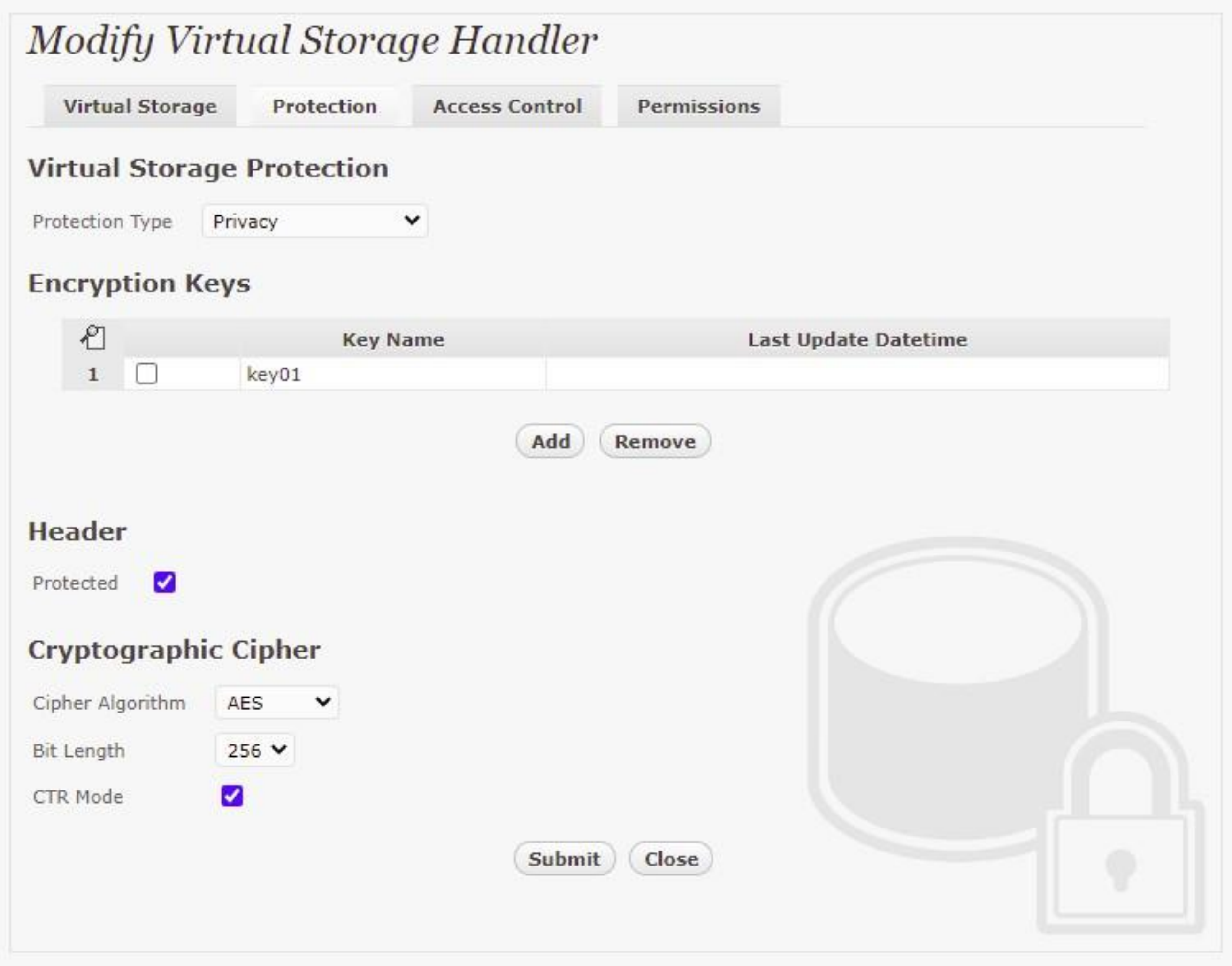
and secure the Microsoft Storage Server storage backend using

```
AES 256-bit
```

encryption and encryption key

```
key01
```

managed at HashiCorp Vault.



Modify Virtual Storage Handler

Virtual Storage Protection

Protection Type: Privacy

Encryption Keys

		Key Name	Last Update Datetime
1	□	key01	

Header

Protected ☑

Cryptographic Cipher

Cipher Algorithm: AES

Bit Length: 256

CTR Mode ☑

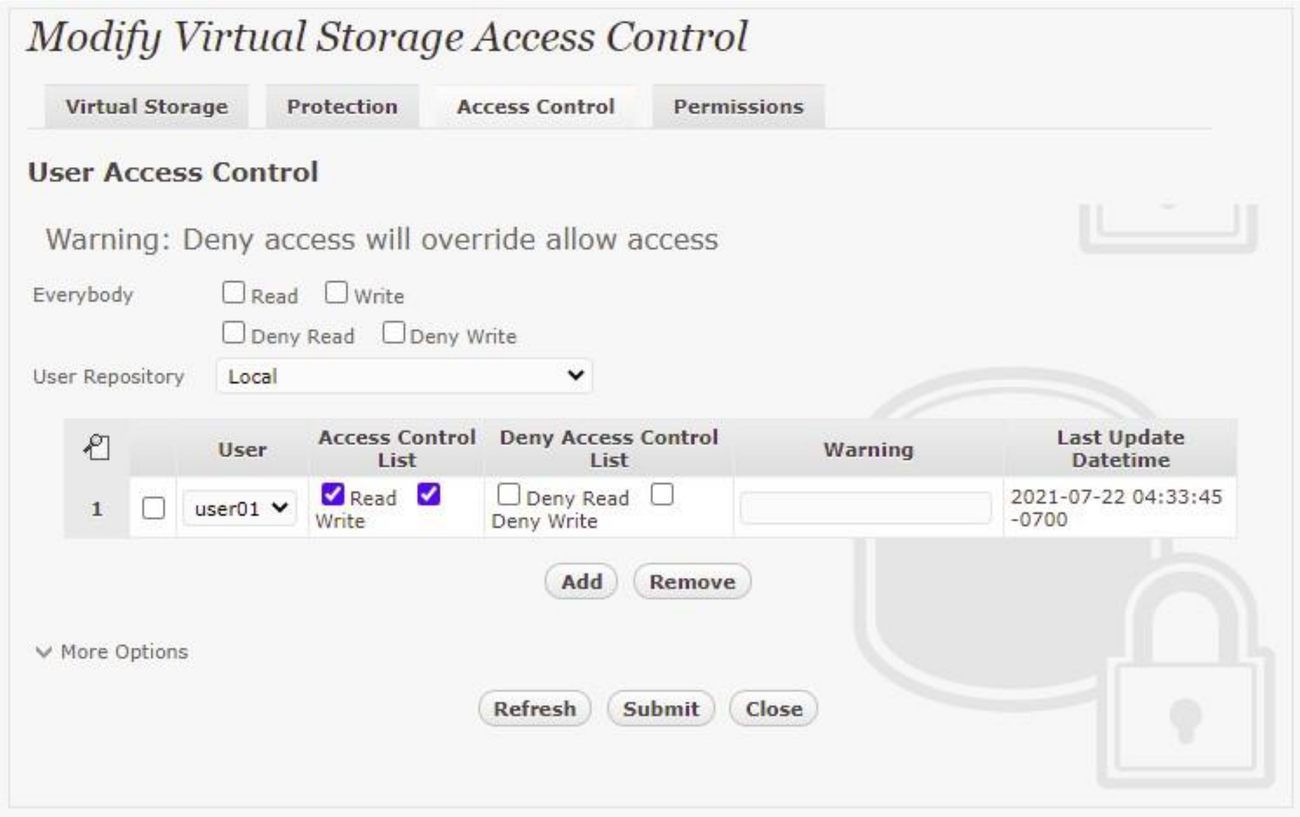
SMB/CIFS storage protocol relies mainly on user-password authentication for access control. In this test, the Bloombase StoreSafe secure storage resource

```
smb01
```

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

Warning: Deny access will override allow access

Everybody □ Read □ Write
□ Deny Read □ Deny Write

User Repository: Local

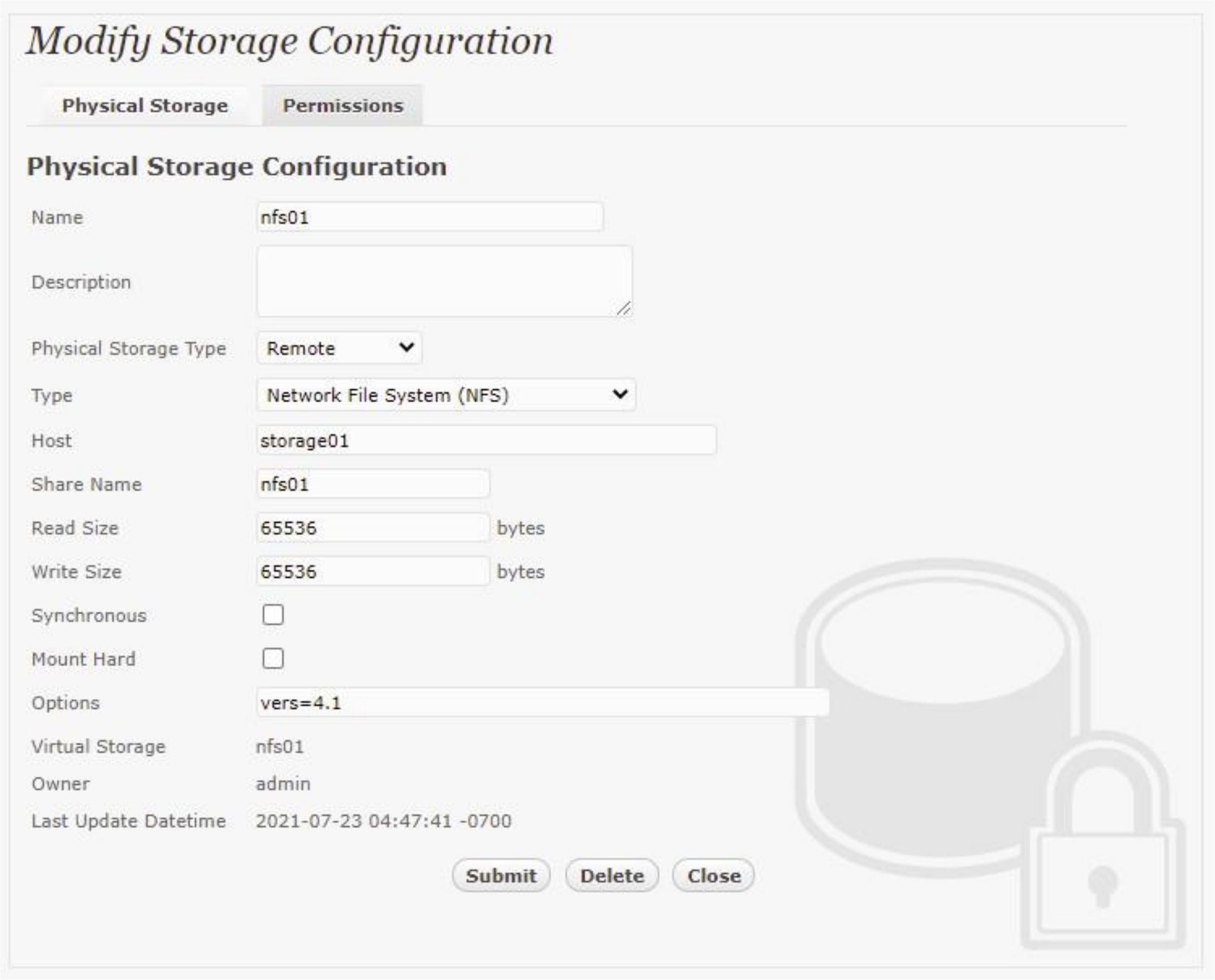
		User	Access Control List	Deny Access Control List	Warning	Last Update Datetime
1	□	user01	☑ Read ☑ Write	□ Deny Read □ Deny Write		2021-07-22 04:33:45 -0700

Data-at-Rest Encryption for NFS

Physical storage namely

```
nfs01
```

is configured to be secured by Bloombase StoreSafe using encryption.



Physical Storage Configuration

Name	nfs01
Description	
Physical Storage Type	Remote
Type	Network File System (NFS)
Host	storage01
Share Name	nfs01
Read Size	65536 bytes
Write Size	65536 bytes
Synchronous	□
Mount Hard	□
Options	vers=4.1
Virtual Storage	nfs01
Owner	admin
Last Update Datetime	2021-07-23 04:47:41 -0700

Virtual storage namely

```
nfs01
```

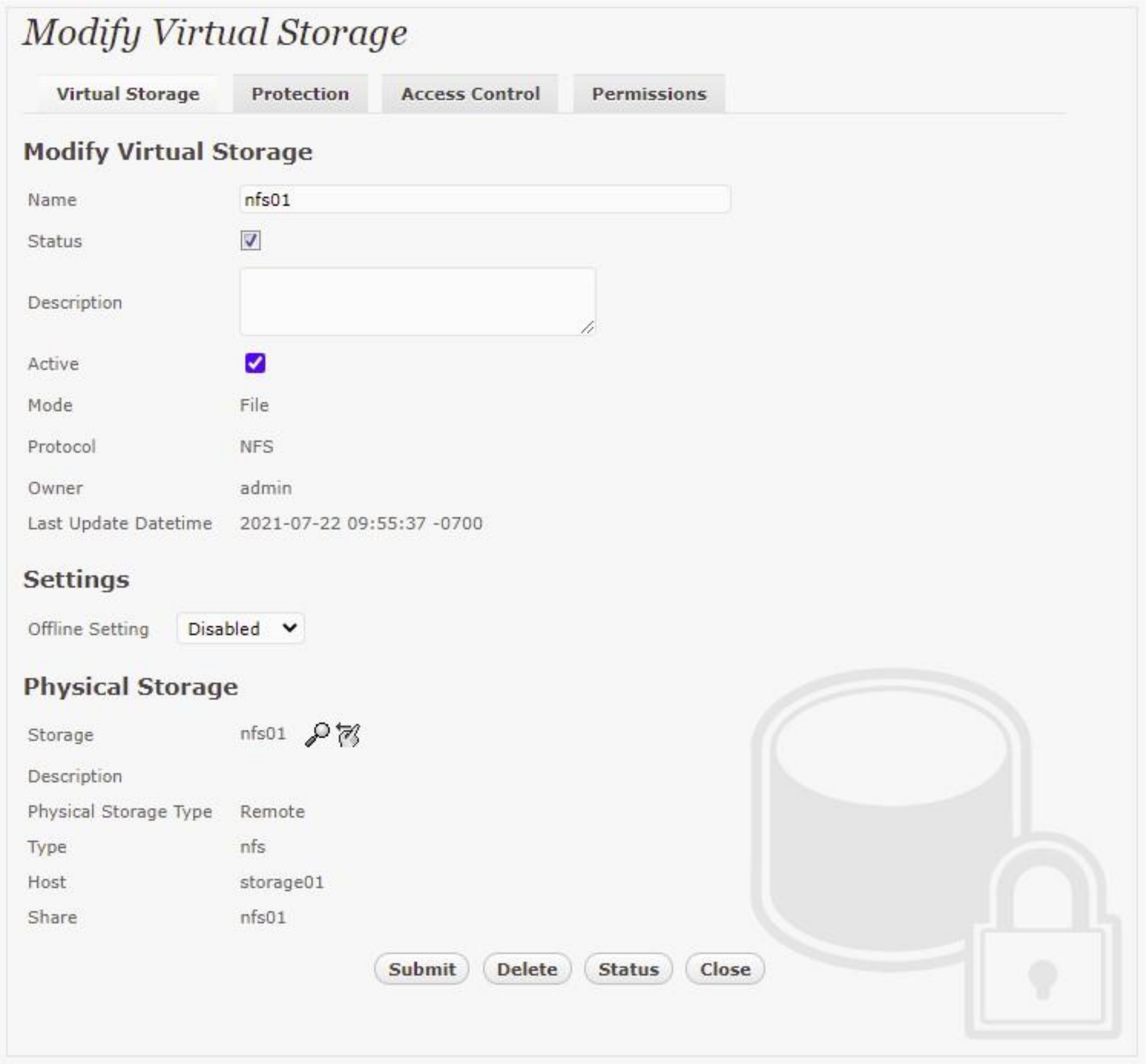
of type

```
File
```

is created to virtualize physical storage

```
nfs01
```

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



Modify Virtual Storage

Name	nfs01
Status	☑
Description	
Active	☑
Mode	File
Protocol	NFS
Owner	admin
Last Update Datetime	2021-07-22 09:55:37 -0700

Settings

Offline Setting: Disabled

Physical Storage

Storage	nfs01
Description	
Physical Storage Type	Remote
Type	nfs
Host	storage01
Share	nfs01

Protection type is specified as

```
Privacy
```

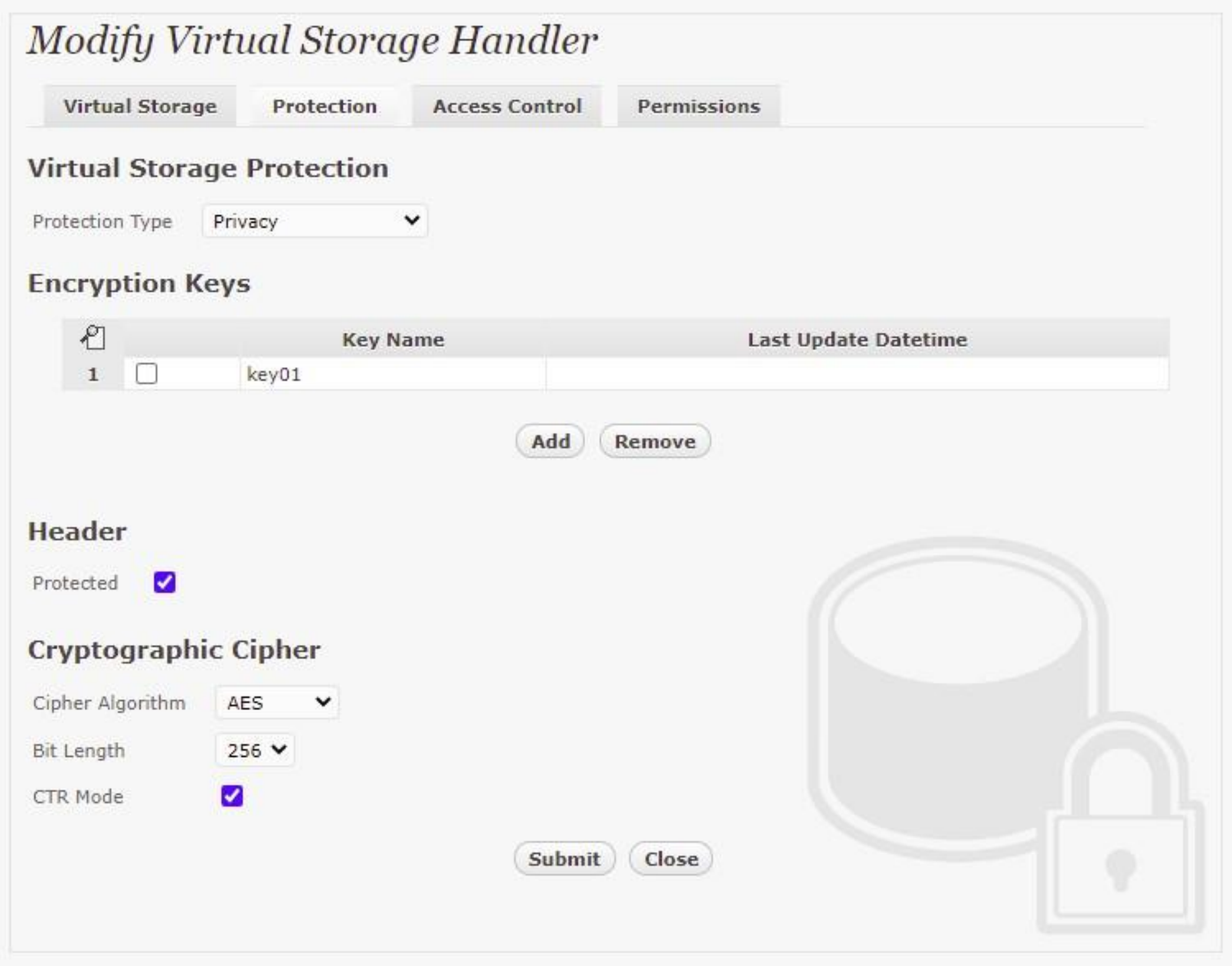
and secure the Microsoft Storage Server storage backend using

```
AES 256-bit
```

encryption and encryption key

```
key01
```

managed at HashiCorp Vault.



Modify Virtual Storage Handler

Virtual Storage Protection

Protection Type: Privacy

Encryption Keys

		Key Name	Last Update Datetime
1	□	key01	

Header

Protected ☑

Cryptographic Cipher

Cipher Algorithm: AES

Bit Length: 256

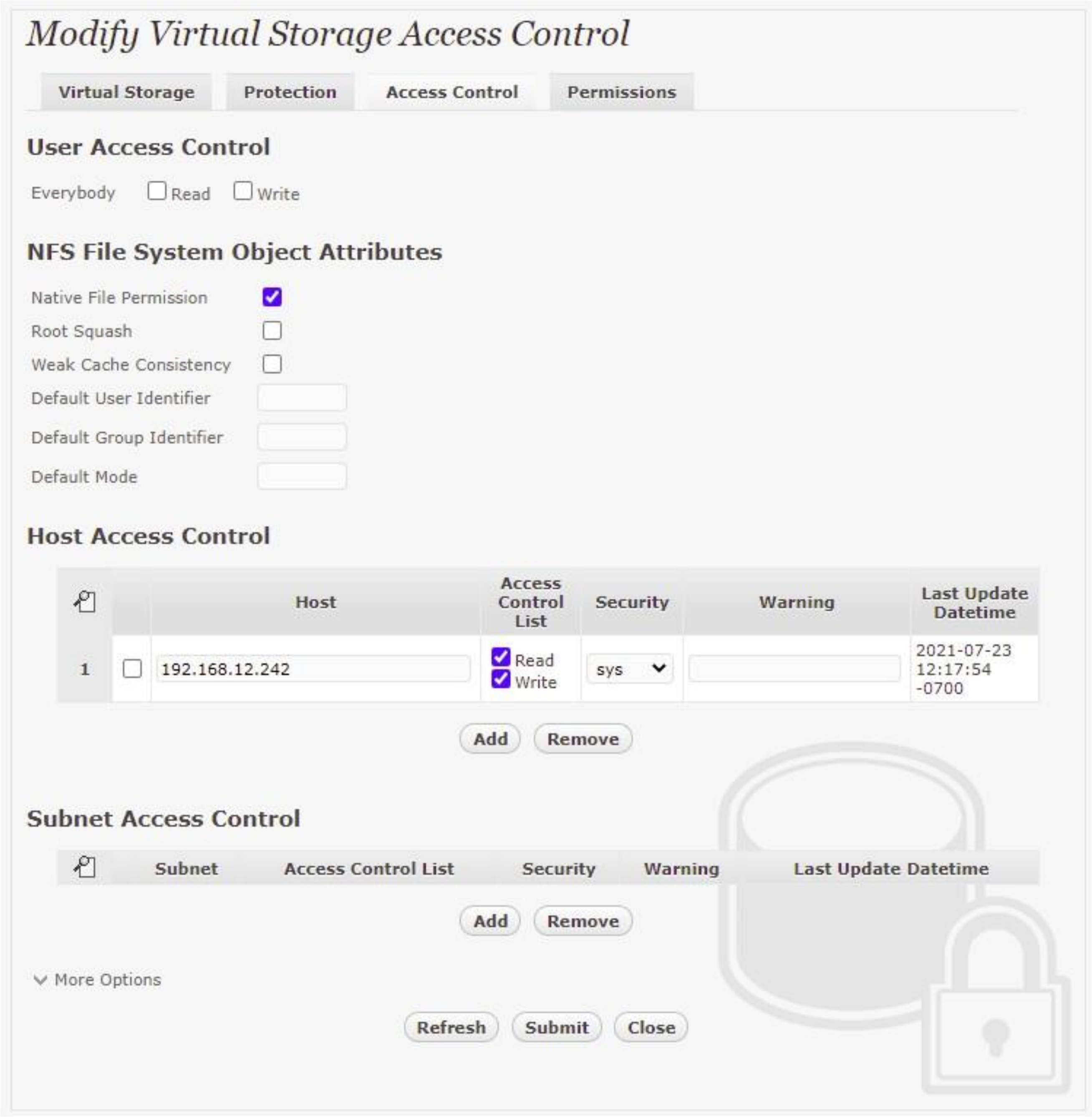
CTR Mode ☑

NFS storage protocol relies mainly on UID/GID and networking for access control. In this test, the Bloombase StoreSafe secure storage resource

```
nfs01
```

is provisioned for client IP

```
192.168.12.242
```



Modify Virtual Storage Access Control

User Access Control

Everybody □ Read □ Write

NFS File System Object Attributes

Native File Permission	☑
Root Squash	□
Weak Cache Consistency	□
Default User Identifier	
Default Group Identifier	
Default Mode	

Host Access Control

		Host	Access Control List	Security	Warning	Last Update Datetime
1	□	192.168.12.242	☑ Read ☑ Write	sys		2021-07-23 12:17:54 -0700

Subnet Access Control

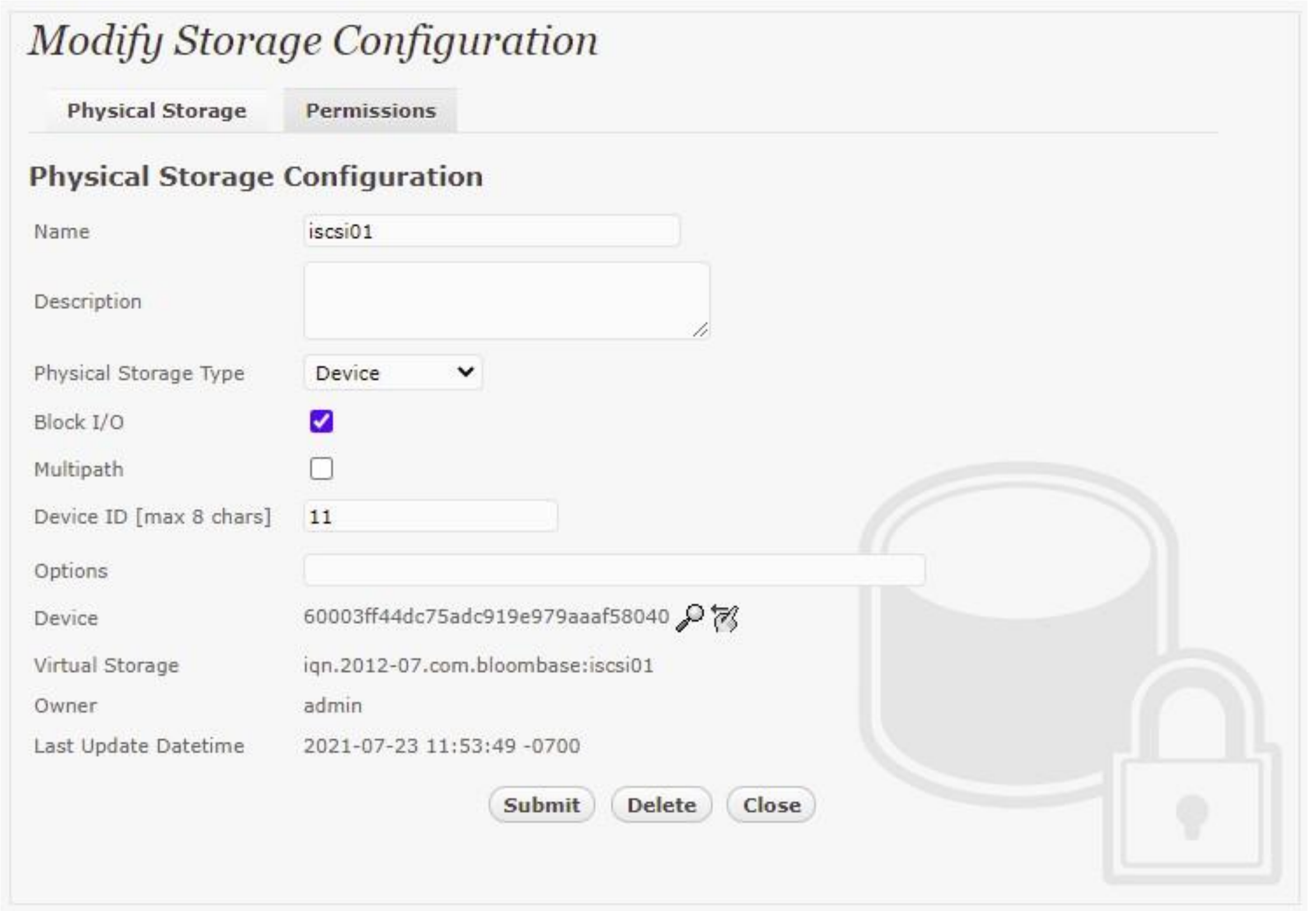
	Subnet	Access Control List	Security	Warning	Last Update Datetime

Data-at-Rest Encryption for iSCSI

Physical storage namely

```
iscsi01
```

is configured to be secured by Bloombase StoreSafe using encryption.



Modify Storage Configuration

Physical Storage Configuration

Name	iscsi01
Description	
Physical Storage Type	Device
Block I/O	☑
Multipath	☐
Device ID [max 8 chars]	11
Options	
Device	60003ff44dc75adc919e979aaaf58040
Virtual Storage	iqn.2012-07.com.bloombase:iscsi01
Owner	admin
Last Update Datetime	2021-07-23 11:53:49 -0700

Virtual storage namely

```
iqn.2012-07.com.bloombase:iscsi01
```

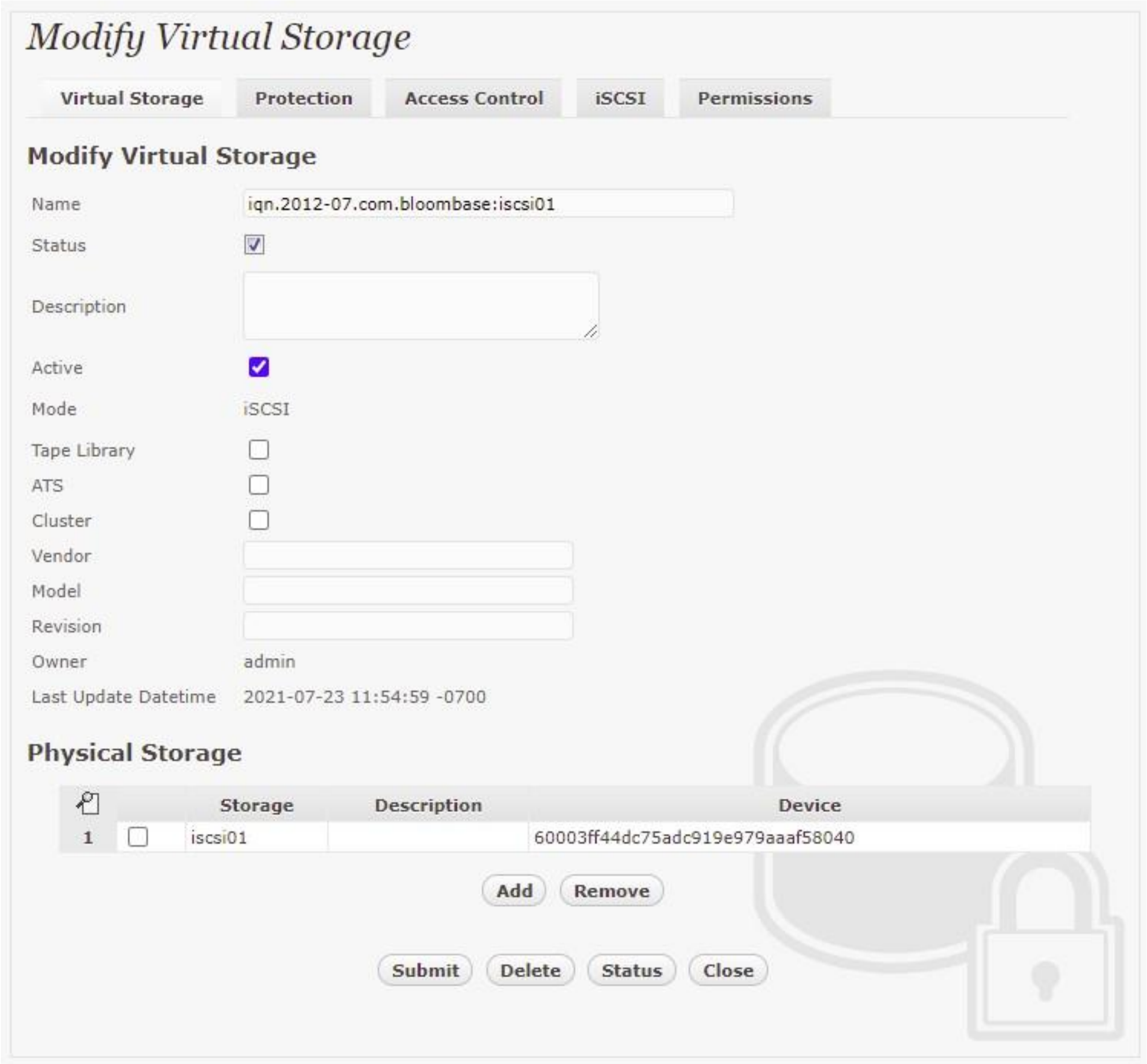
of type

```
iSCSI
```

is created to virtualize physical storage

```
iscsi01
```

for application transparent encryption protection over network file protocols including iSCSI.



Modify Virtual Storage

Name	iqn.2012-07.com.bloombase:iscsi01
Status	☑
Description	
Active	☑
Mode	iSCSI
Tape Library	☐
ATS	☐
Cluster	☐
Vendor	
Model	
Revision	
Owner	admin
Last Update Datetime	2021-07-23 11:54:59 -0700

Physical Storage

		Storage	Description	Device
1	☐	iscsi01		60003ff44dc75adc919e979aaaf58040

Protection type is specified as

```
Privacy
```

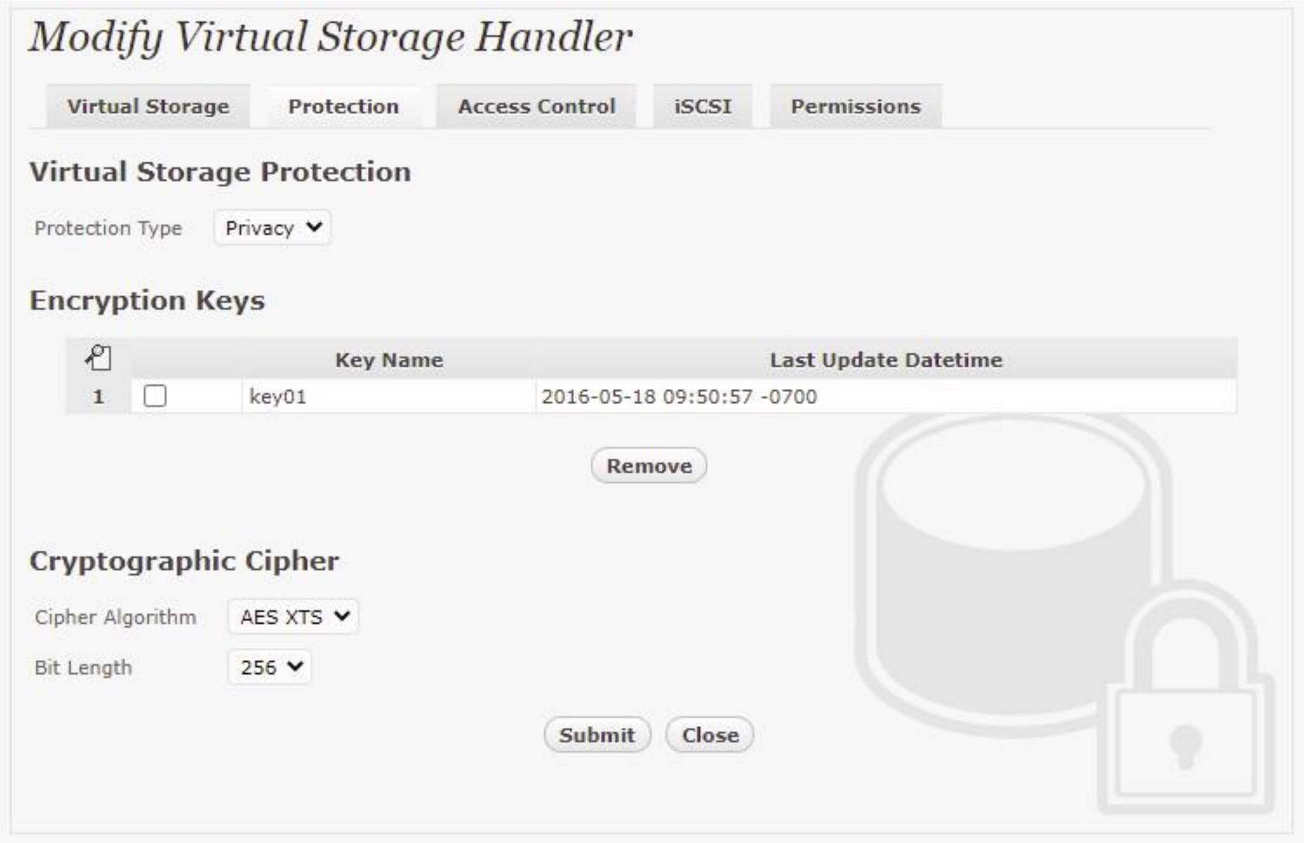
and secure the Microsoft Storage Server storage backend using

```
AES XTS 256-bit
```

encryption and encryption key

```
key01
```

managed at HashiCorp Vault.



Modify Virtual Storage Handler

Virtual Storage Protection

Protection Type: Privacy

Encryption Keys

		Key Name	Last Update Datetime
1	□	key01	2016-05-18 09:50:57 -0700

Cryptographic Cipher

Cipher Algorithm: AES XTS

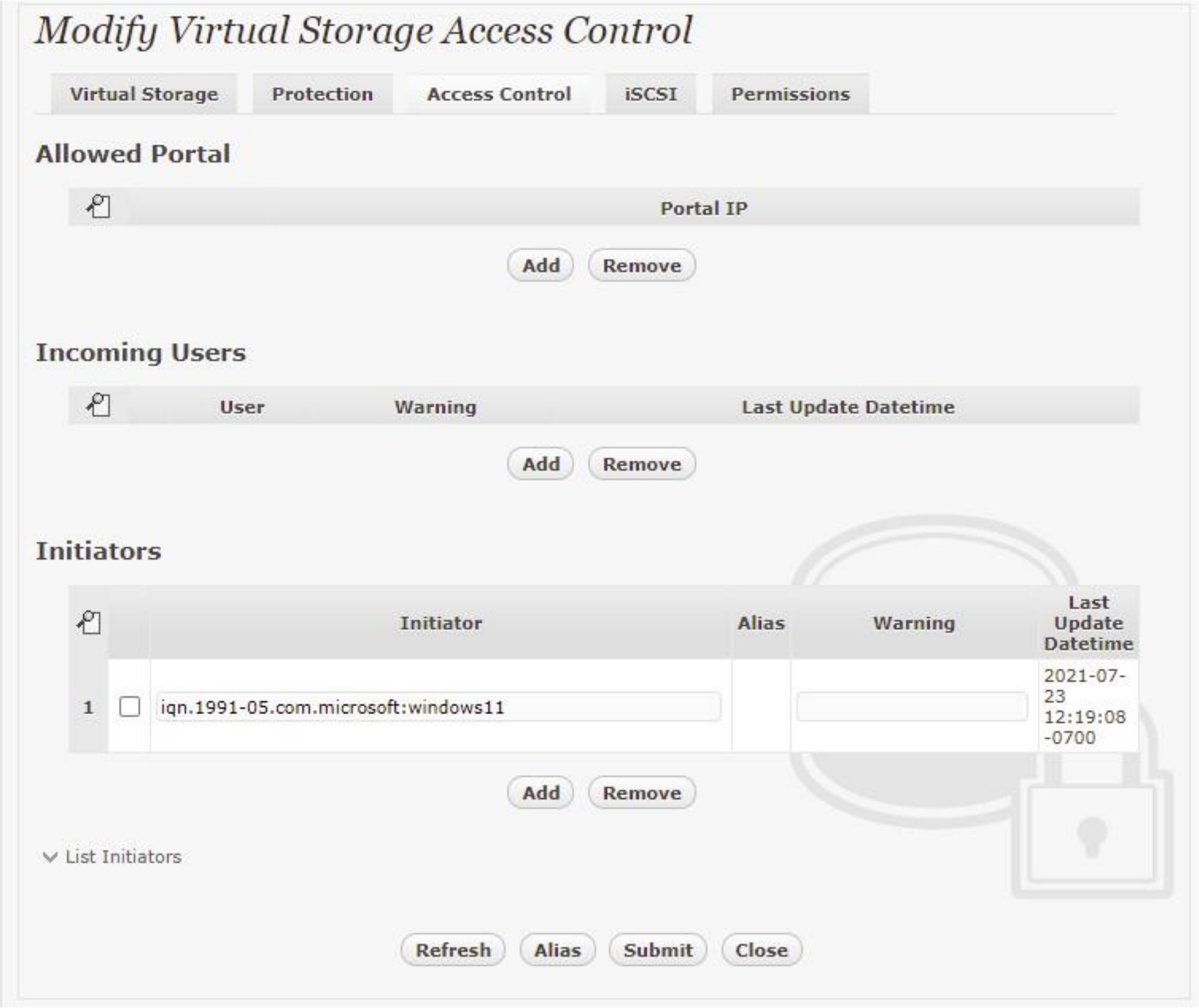
Bit Length: 256

iSCSI storage protocol relies mainly on CHAP, IQN, and networking for access control. In this test, the Bloombase StoreSafe secure storage resource

```
iqn.2012-07.com.bloombase:iscsi01
```

is provisioned for initiator

```
iqn.1991-05.com.microsoft:windows11
```



Modify Virtual Storage Access Control

Allowed Portal

	Portal IP

Incoming Users

	User	Warning	Last Update Datetime

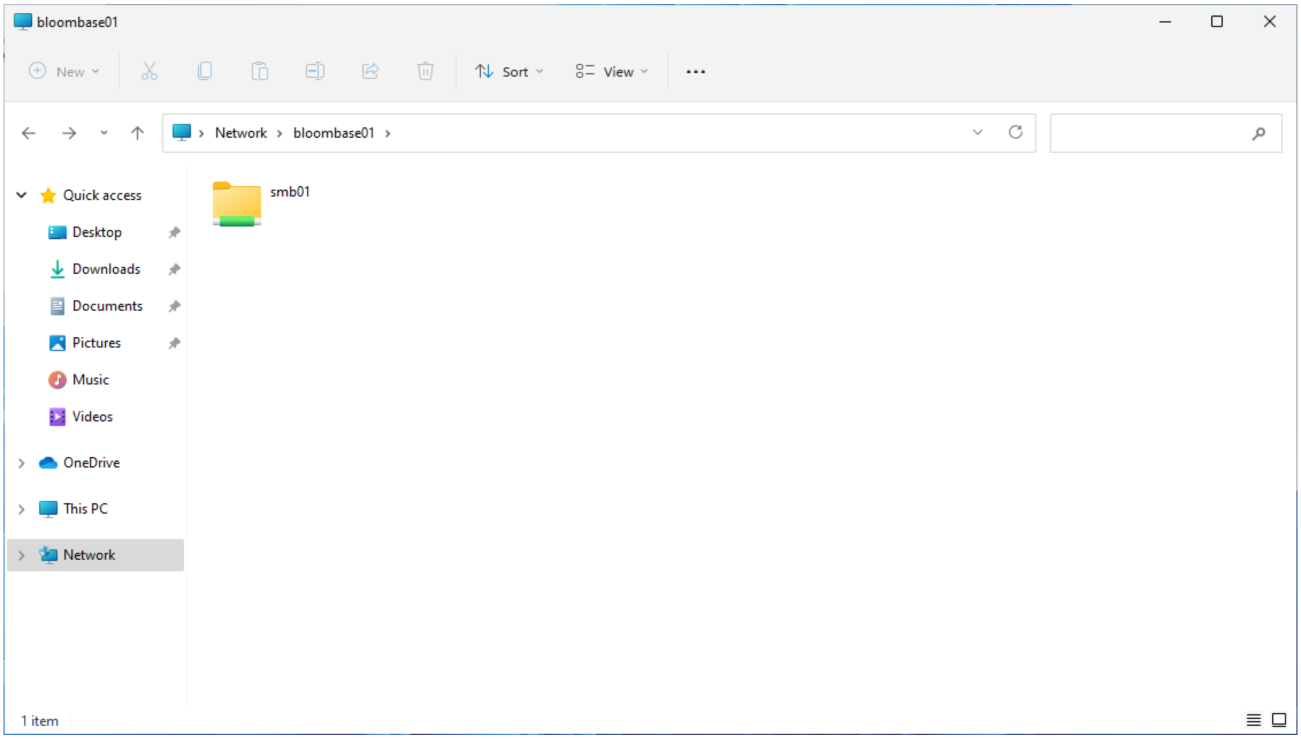
Initiators

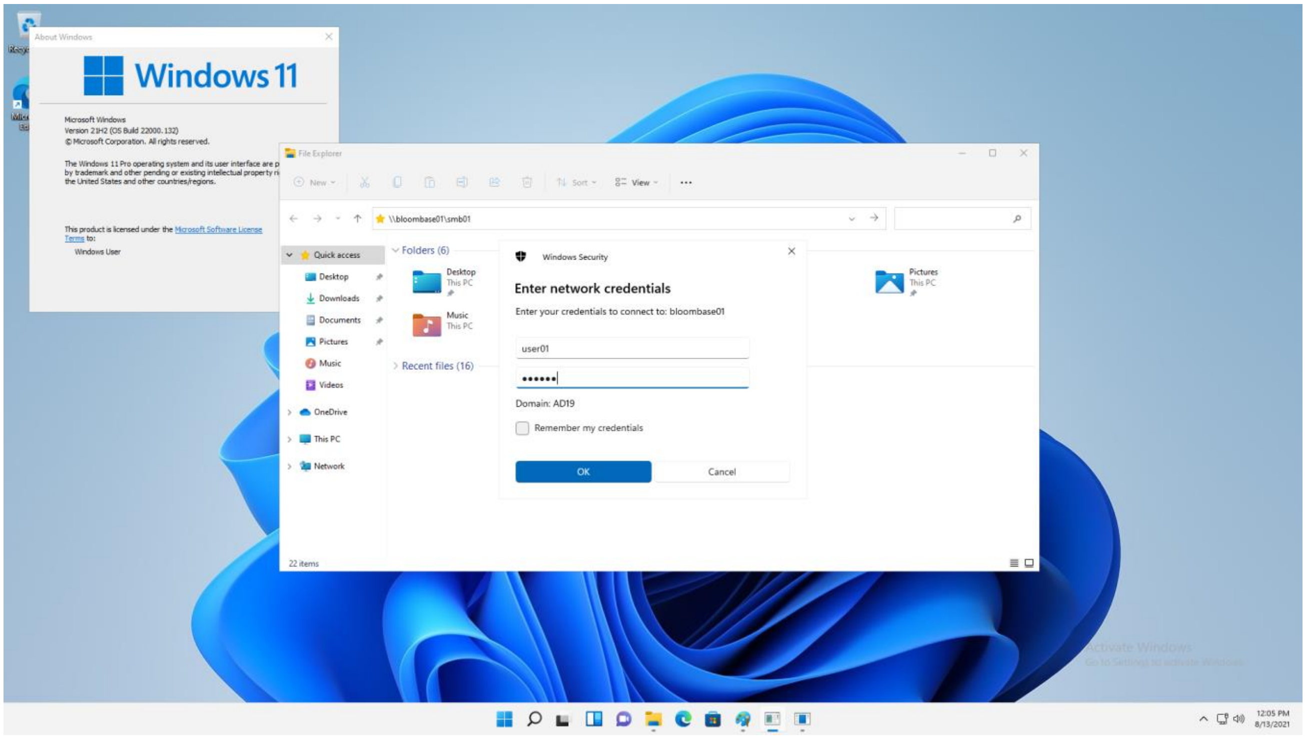
		Initiator	Alias	Warning	Last Update Datetime
1	□	iqn.1991-05.com.microsoft:windows11			2021-07-23 12:19:08 -0700

Use Cases

Data-at-Rest Encryption for SMB

SMB shares are an example from the many protocols Bloombase StoreSafe supports for encryption. A share from a Windows Server 2022 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.




About Windows

Windows 11

Microsoft Windows
Version 21H2 (OS Build 22000.132)
© Microsoft Corporation. All rights reserved.

The Windows 11 Pro operating system and its user interface are p
by trademark and other pending or existing intellectual property ri
the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:
Windows User

\\bloombase01\smb01

Windows Security

Enter network credentials

Enter your credentials to connect to: bloombase01

user01

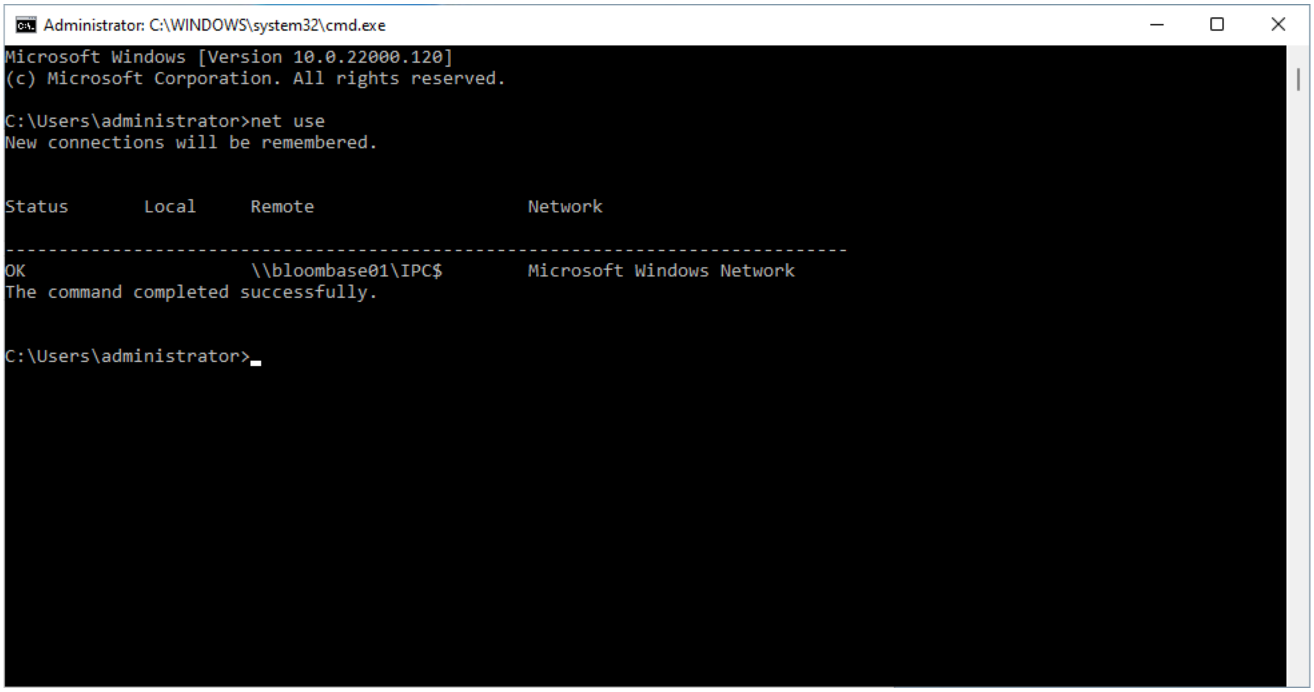
••••••

Domain: AD19

□ Remember my credentials

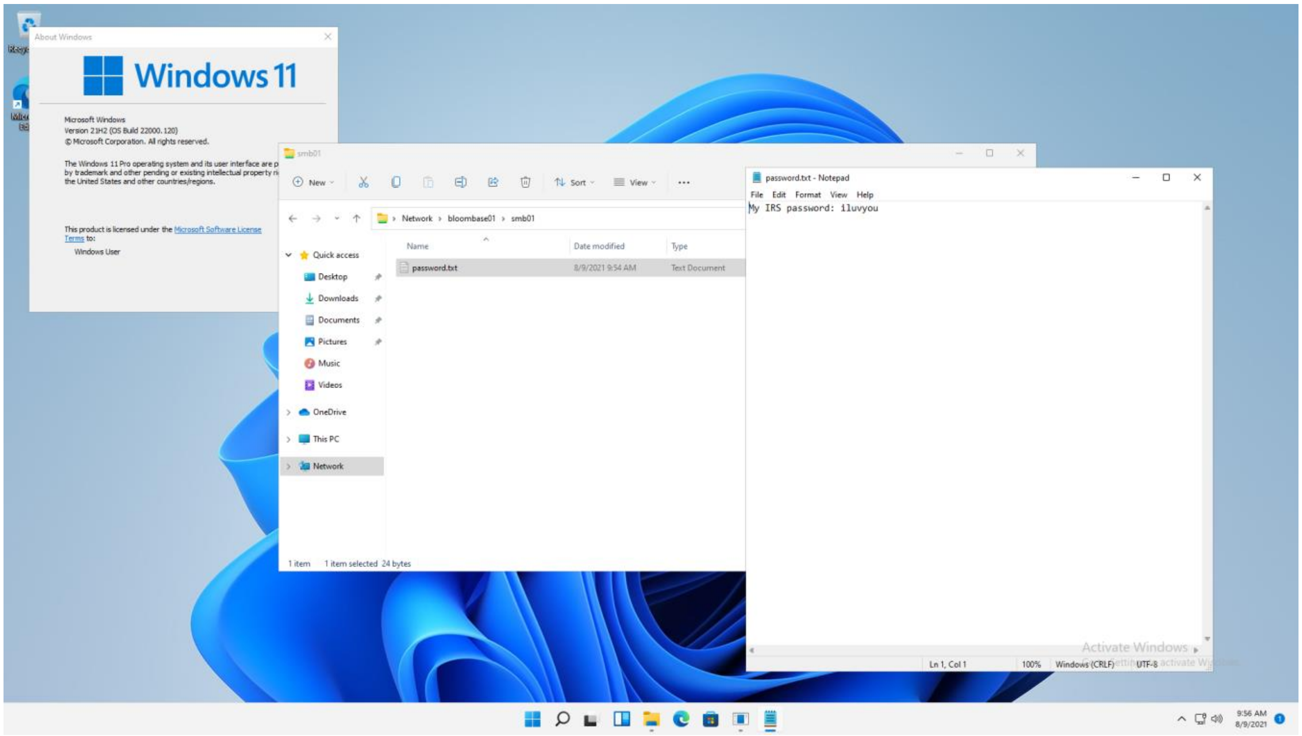
OK Cancel

Windows 11 clients can use the included network share on file manager to access the SMB share. Data owners can alternatively use the Net Use command to specify additional mounting options.



```
Microsoft Windows [Version 10.0.22000.120]
(c) Microsoft Corporation. All rights reserved.

C:\Users\administrator>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK                     \\bloombase01\IPC$        Microsoft Windows Network
The command completed successfully.


C:\Users\administrator>_
```

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 2022 backend share.



Microsoft Windows
Version 21H2 (OS Build 22000.120)
© Microsoft Corporation. All rights reserved.

The Windows 11 Pro operating system and its user interface are p by trademark and other pending or existing intellectual property ri the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:
Windows User

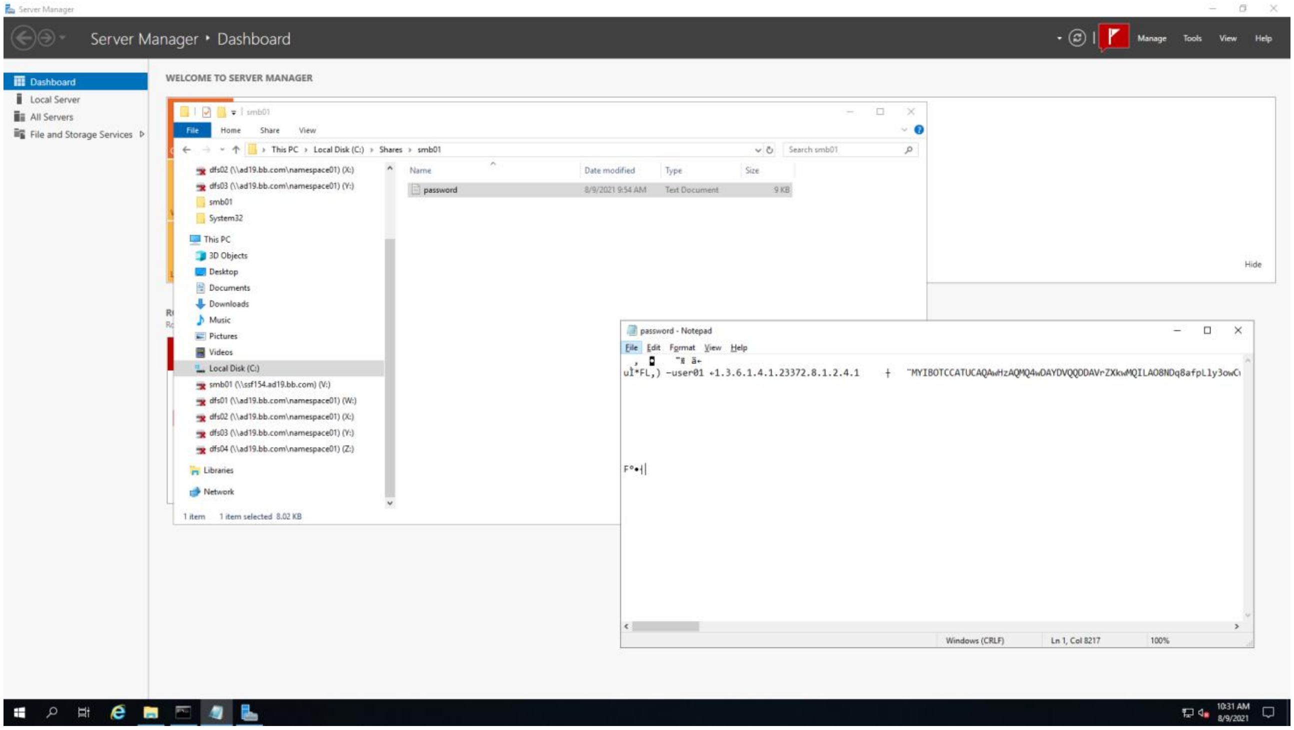
Name	Date modified	Type
password.txt	8/9/2021 9:54 AM	Text Document

1 item 1 item selected 24 bytes

```
My IRS password: iluvyou
```

Ln 1, Col 1 100% Windows (CRLF) UTF-8

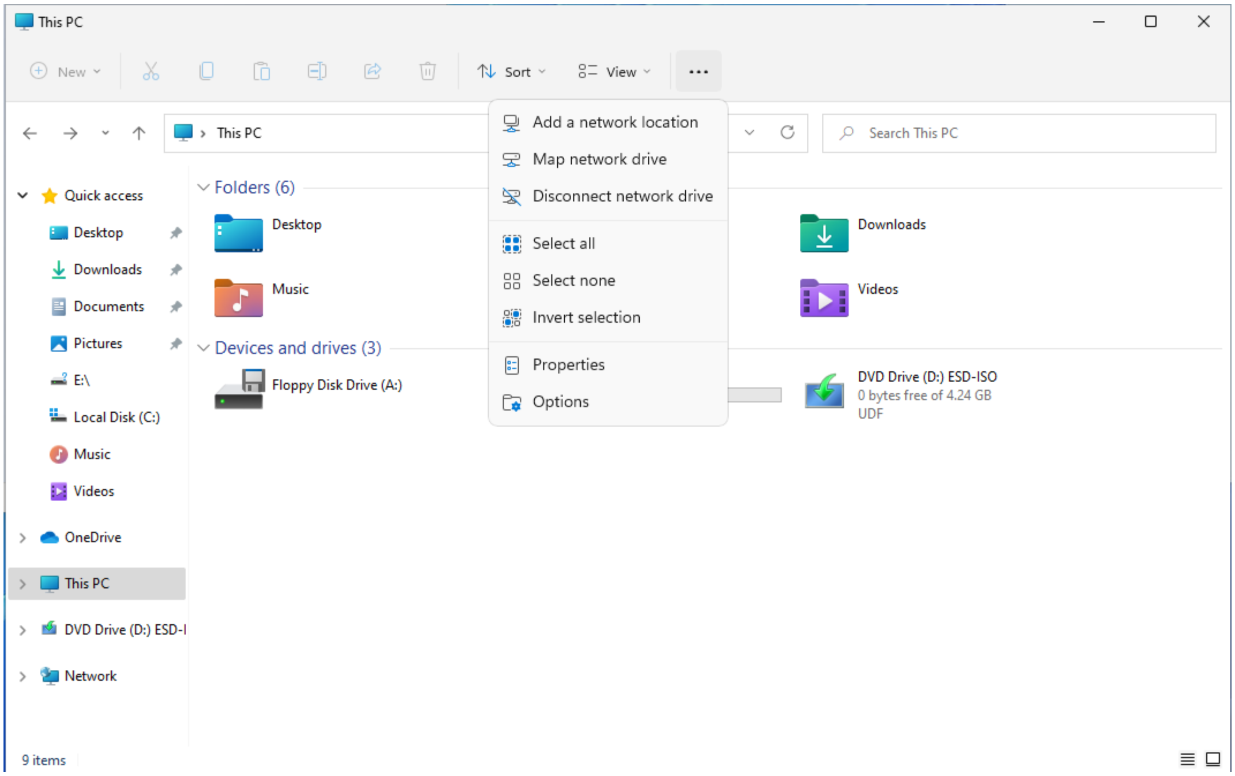
If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.

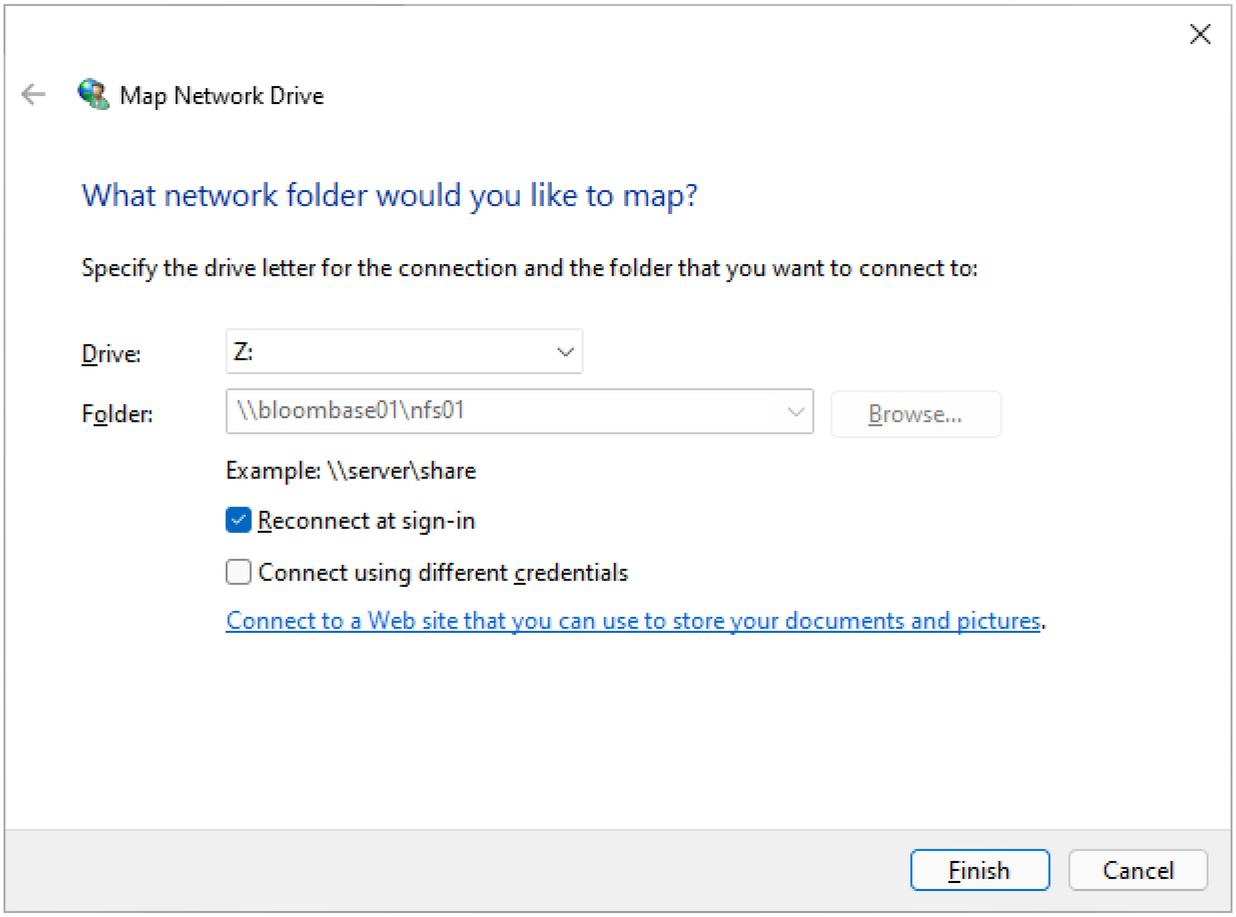

Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
smb01
File Home Share View
This PC › Local Disk (C:) › Shares › smb01
Search smb01
dfs02 (\\ad19.bb.com\namespace01) (X:)
dfs03 (\\ad19.bb.com\namespace01) (Y:)
smb01
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
smb01 (\\ssf154.ad19.bb.com) (V:)
dfs01 (\\ad19.bb.com\namespace01) (W:)
dfs02 (\\ad19.bb.com\namespace01) (X:)
dfs03 (\\ad19.bb.com\namespace01) (Y:)
dfs04 (\\ad19.bb.com\namespace01) (Z:)
Libraries
Network
Name Date modified Type Size
password 8/9/2021 9:54 AM Text Document 9 KB
1 item 1 item selected 8.02 KB
Hide
password - Notepad
File Edit Format View Help
Windows (CRLF) Ln 1, Col 8217 100%
10:31 AM 8/9/2021

```
  ,  ◘    ˜ã ã←
uÌ*FL,) -user01 ←1.3.6.1.4.1.23372.8.1.2.4.1    ┼   ˜MYIBOTCCATUCAQAwHzAQMQ4wDAYDVQQDDAVrZXkwMQILAO8NDq8afpLly3owC

F°•┤
```

Data-at-Rest Encryption for NFS

NFS shares are an example from the many protocols Bloombase StoreSafe supports for encryption. A share from a Windows Server 2022 system that is accessible by configure clients 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.


This PC
New
Sort
View
...
This PC
Search This PC
Add a network location
Map network drive
Disconnect network drive
Select all
Select none
Invert selection
Properties
Options
Quick access
Desktop
Downloads
Documents
Pictures
E:\
Local Disk (C:)
Music
Videos
OneDrive
This PC
DVD Drive (D:) ESD-I
Network
Folders (6)
Desktop
Downloads
Music
Videos
Devices and drives (3)
Floppy Disk Drive (A:)
DVD Drive (D:) ESD-ISO
0 bytes free of 4.24 GB
UDF
9 items


Map Network Drive
What network folder would you like to map?
Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\bloombase01\nfs01

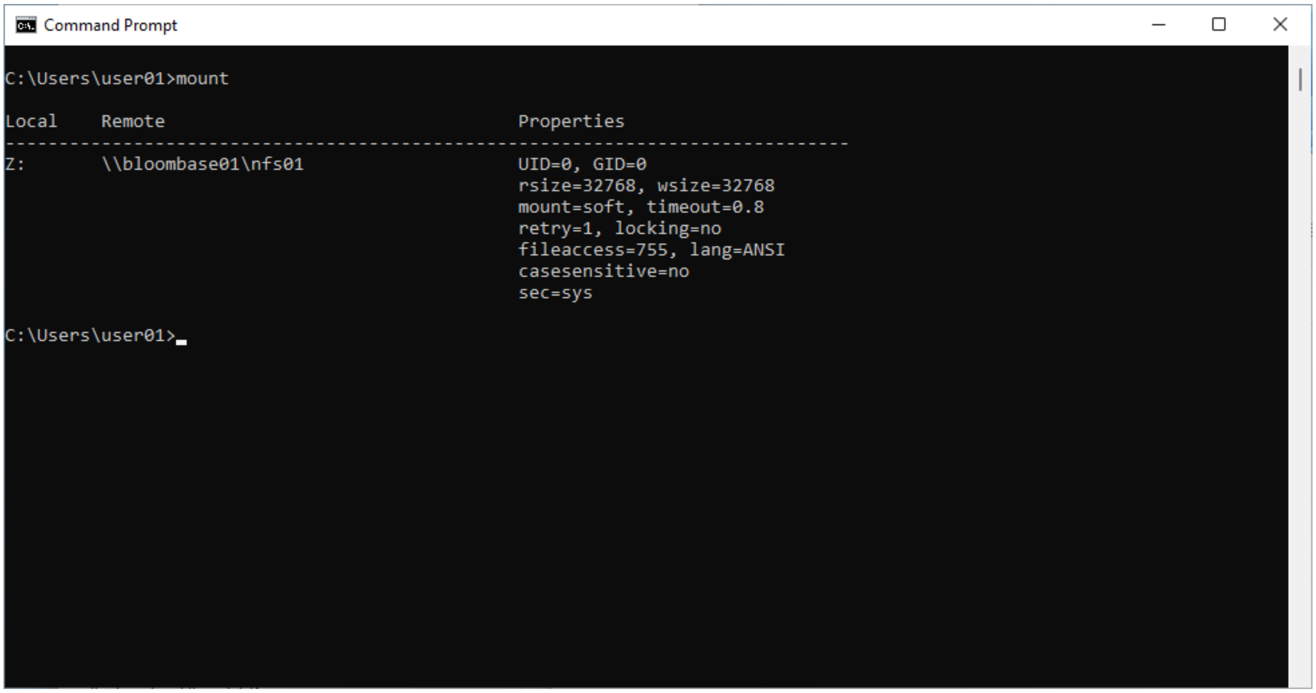
Browse...
Example: \\server\share

☑ Reconnect at sign-in

☐ Connect using different credentials

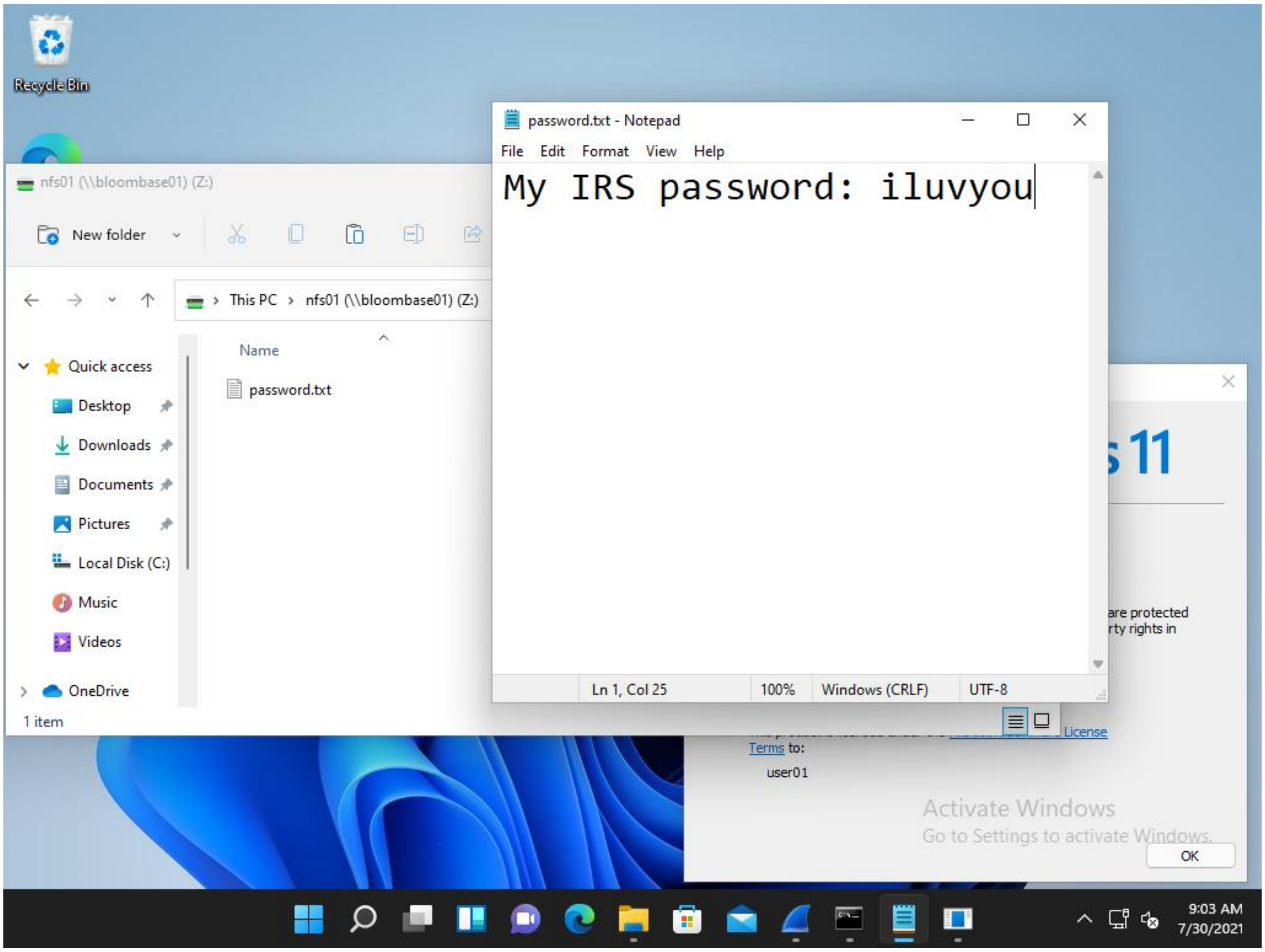
Connect to a Web site that you can use to store your documents and pictures.
Finish
Cancel

Windows 11 clients can use the included map network drive option to add the NFS share with a drive letter. Data owners can alternatively use the mount command to specify additional mounting options.



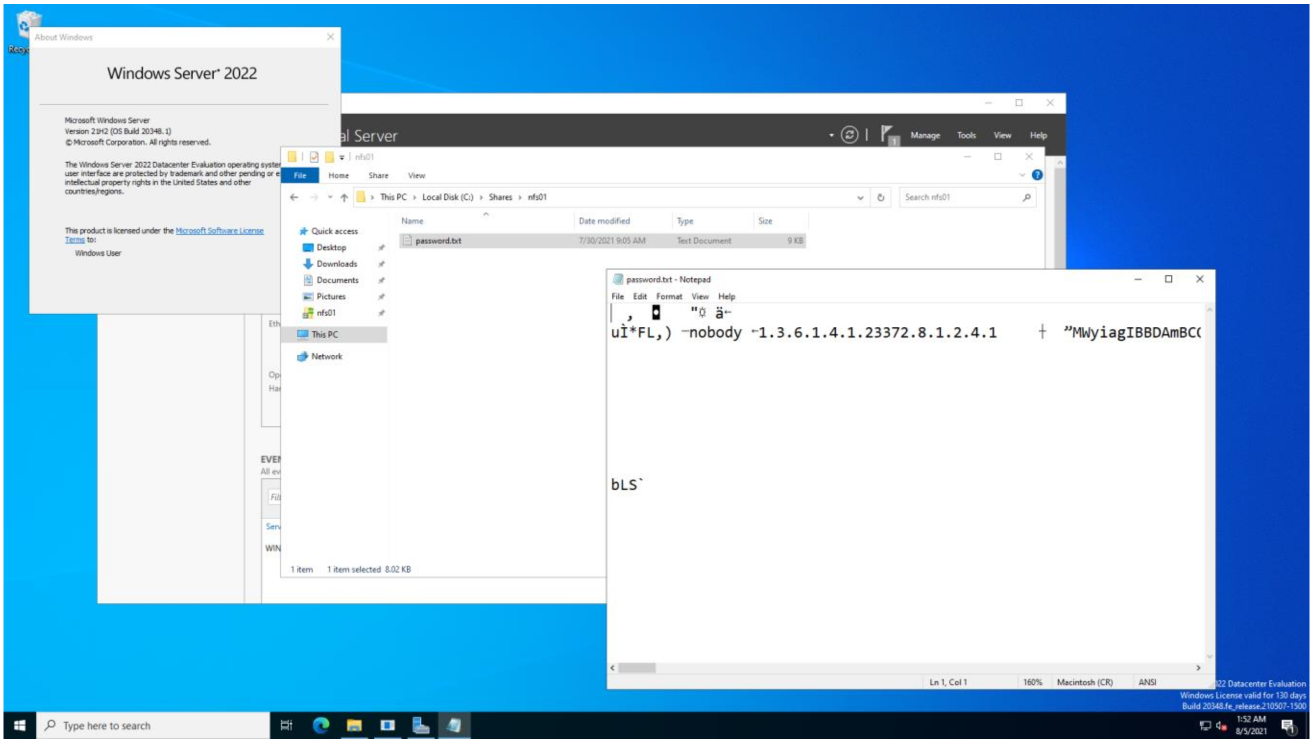
```
C:\Users\user01>mount

Local    Remote                                 Properties
-------------------------------------------------------------------------------
Z:       \\bloombase01\nfs01                    UID=0, GID=0
                                                rsize=32768, wsize=32768
                                                mount=soft, timeout=0.8
                                                retry=1, locking=no
                                                fileaccess=755, lang=ANSI
                                                casesensitive=no
                                                sec=sys

C:\Users\user01>
```

On the demo virtual encrypted NFS 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 2022 backend share.



My IRS password: iluvyou

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.



Microsoft Windows Server
Version 21H2 (OS Build 20348.1)
© Microsoft Corporation. All rights reserved.

The Windows Server 2022 Datacenter Evaluation operating syster
user interface are protected by trademark and other pending or e
intellectual property rights in the United States and other
countries/regions.

This product is licensed under the Microsoft Software License Terms to:
Windows User

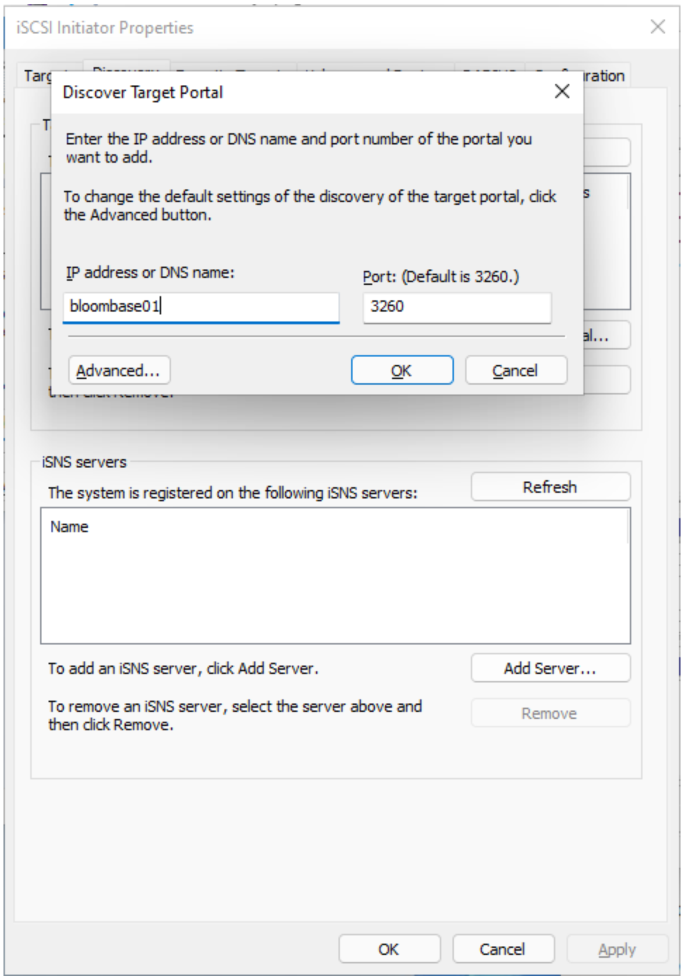
Name	Date modified	Type	Size
password.txt	7/30/2021 9:05 AM	Text Document	9 KB

```
 ,  ●    "☼ ä←
uÌ*FL,) ¬nobody ←1.3.6.1.4.1.23372.8.1.2.4.1     ┼  ”MWyiagIBBDAmBC(





bLS`
```

Windows Server 2022 Datacenter Evaluation
Windows License valid for 130 days
Build 20348.fe_release.210507-1500

Data-at-Rest Encryption for iSCSI

iSCSI targets are an example from the many protocols Bloombase StoreSafe supports for encryption. A target from a Windows Server 2022 system that is accessible by configure clients 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.



Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

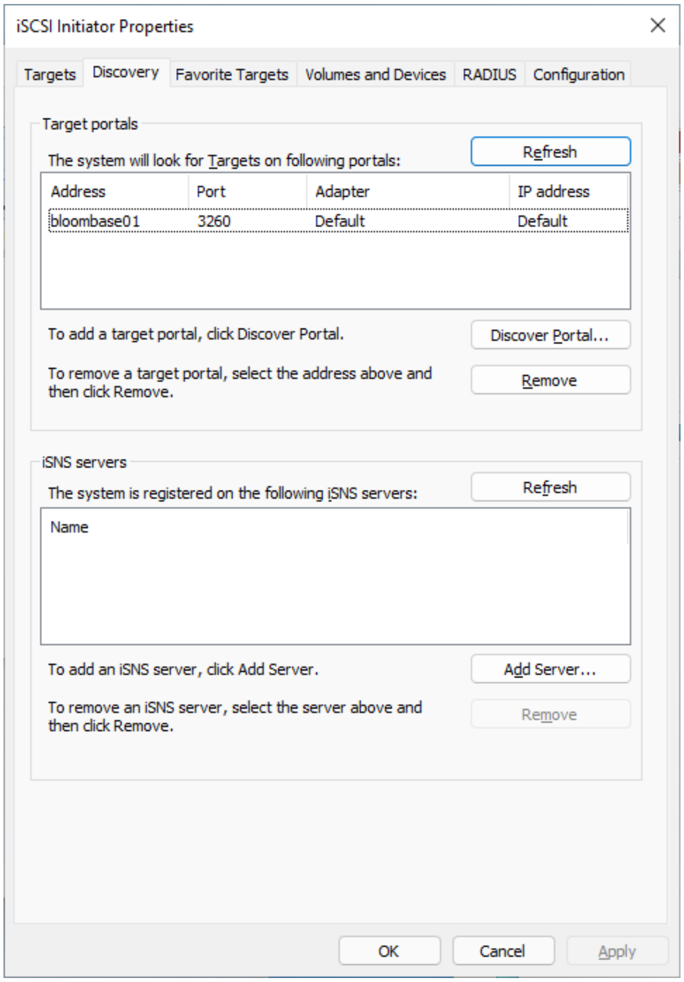
IP address or DNS name: bloombase01

Port: (Default is 3260.) 3260

The system is registered on the following iSNS servers:

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click Remove.



The system will look for Targets on following portals:

Address	Port	Adapter	IP address
bloombase01	3260	Default	Default

To add a target portal, click Discover Portal.

To remove a target portal, select the address above and then click Remove.

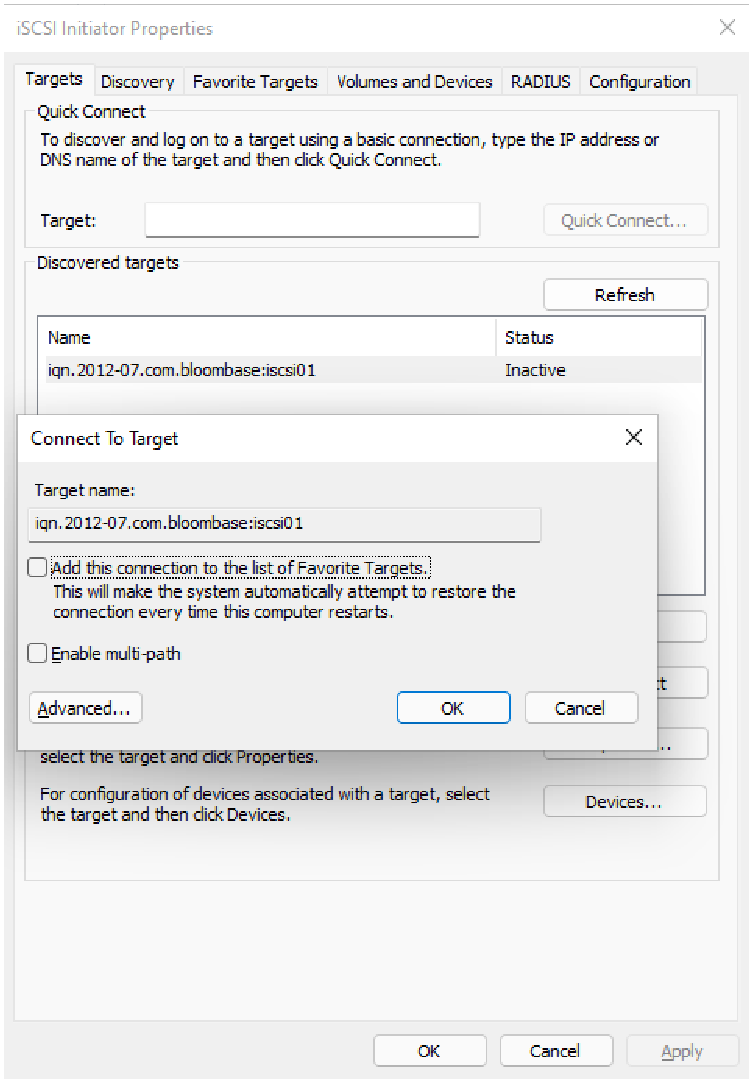
The system is registered on the following iSNS servers:

Name

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click Remove.

Windows 11 clients can attach the virtual encrypted share with the default iSCSI initiator tool. Add the hostname and port to the discover tab, then connect to the Bloombase StoreSafe target. To access the iSCSI disk, make sure the client IQN is be added the Bloombase StoreSafe configuration. The disk will be mounted to the system and it can be formatted with a filesystem.



iSCSI Initiator Properties

Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status
iqn.2012-07.com.bloombase:iscsi01	Inactive

Connect To Target

Target name:

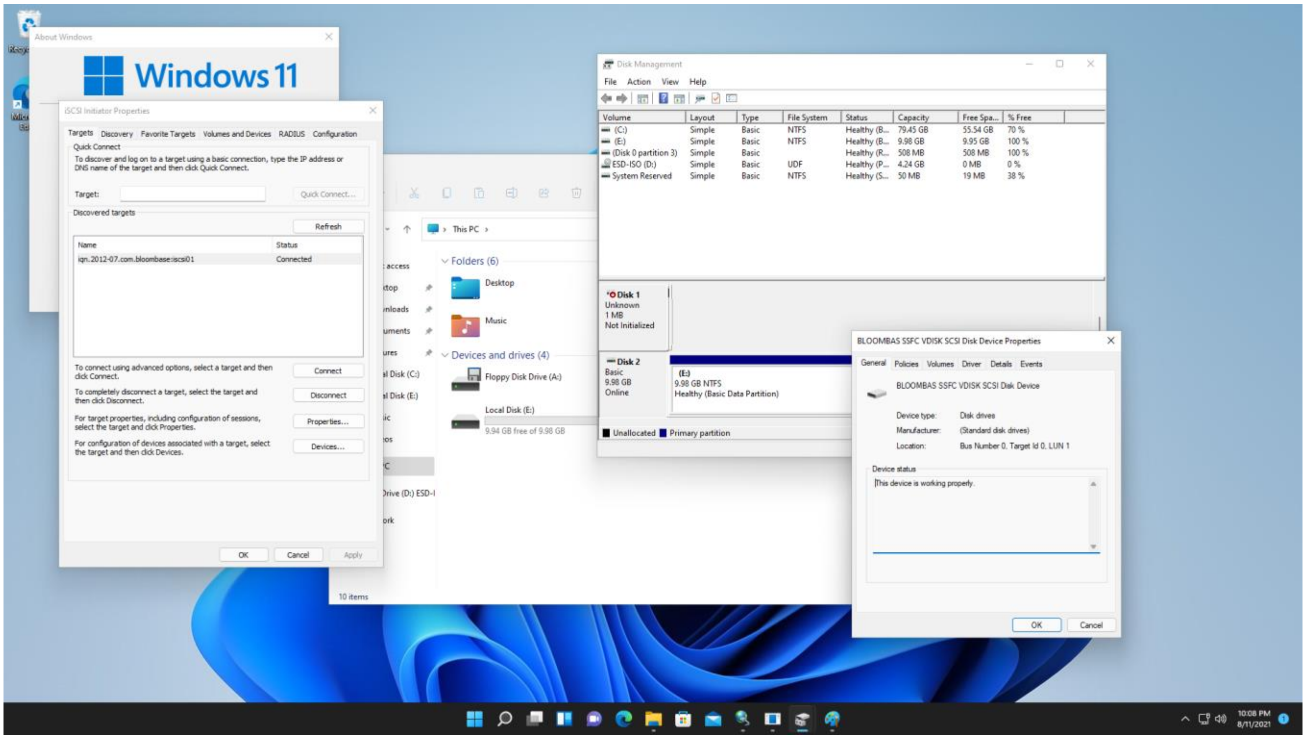
iqn.2012-07.com.bloombase:iscsi01

□ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

□ Enable multi-path

select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.



Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status
iqn.2012-07.com.bloombase:iscsi01	Connected

To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	79.45 GB	55.54 GB	70 %
(E:)	Simple	Basic	NTFS	Healthy (B...	9.98 GB	9.95 GB	100 %
(Disk 0 partition 3)	Simple	Basic		Healthy (R...	508 MB	508 MB	100 %
ESD-ISO (D:)	Simple	Basic	UDF	Healthy (P...	4.24 GB	0 MB	0 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	50 MB	19 MB	38 %

Disk 1
Unknown
1 MB
Not Initialized

Disk 2
Basic
9.98 GB
Online

(E:)
9.98 GB NTFS
Healthy (Basic Data Partition)

■ Unallocated ■ Primary partition

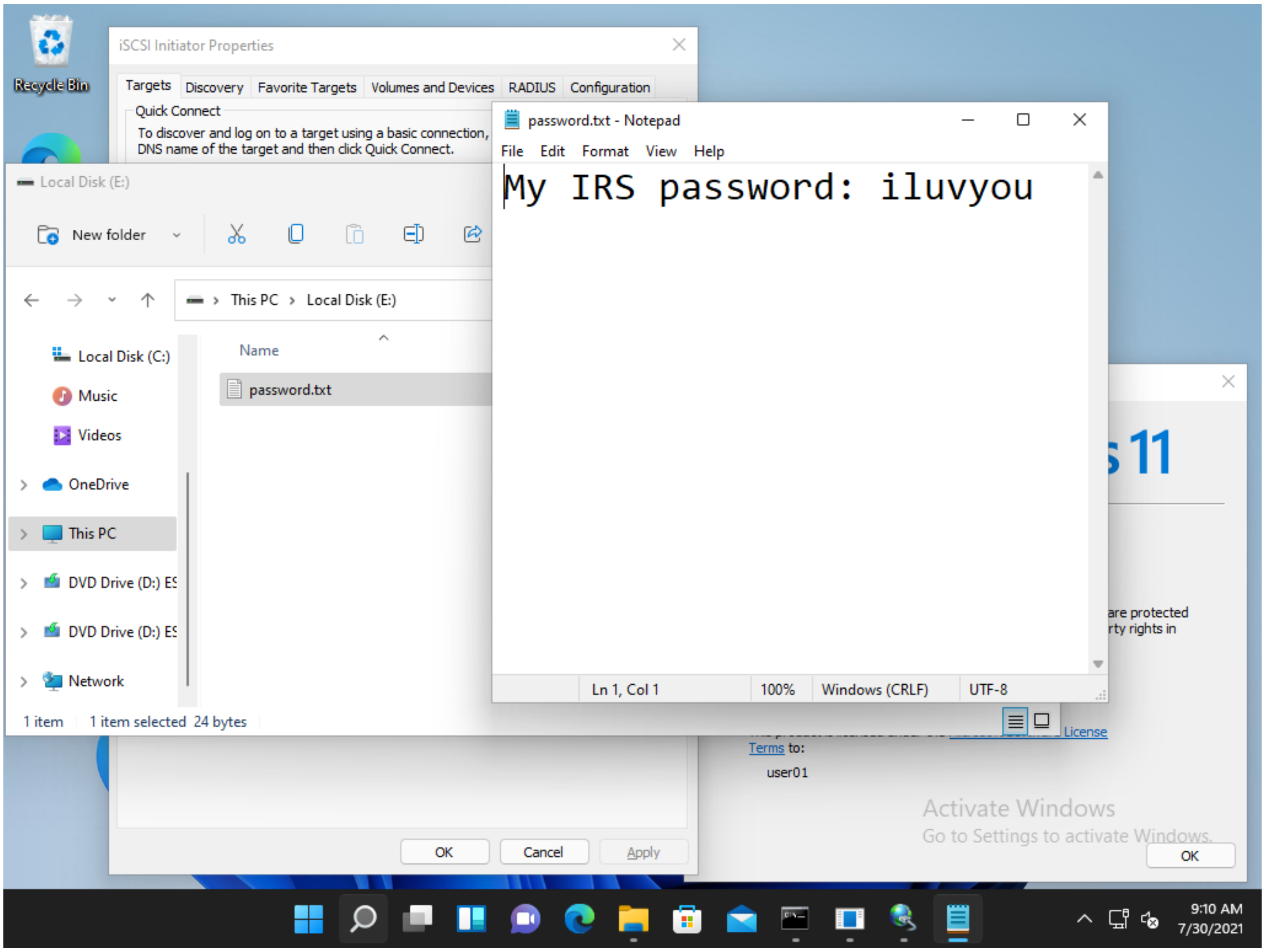
BLOOMBAS SSFC VDISK SCSI Disk Device

Device type: Disk drives
Manufacturer: (Standard disk drives)
Location: Bus Number 0, Target Id 0, LUN 1

Device status

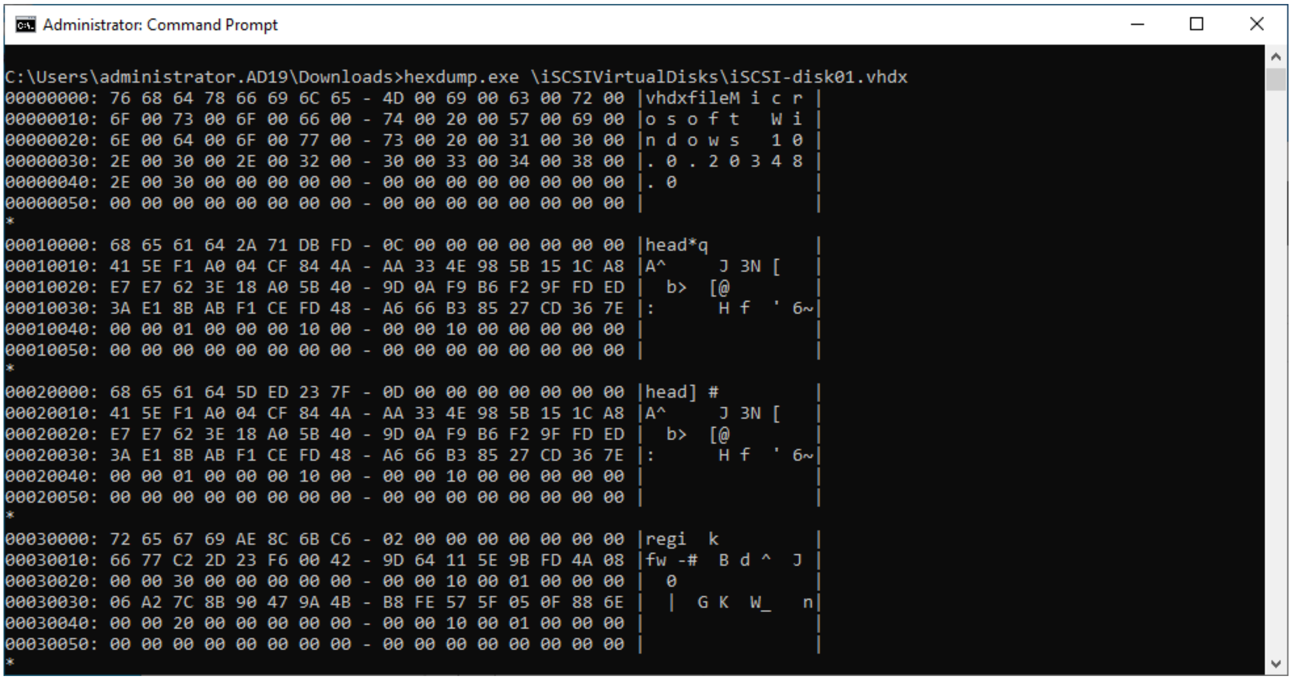
This device is working properly.

On the demo virtual encrypted iSCSI target, 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 2022 backend target.

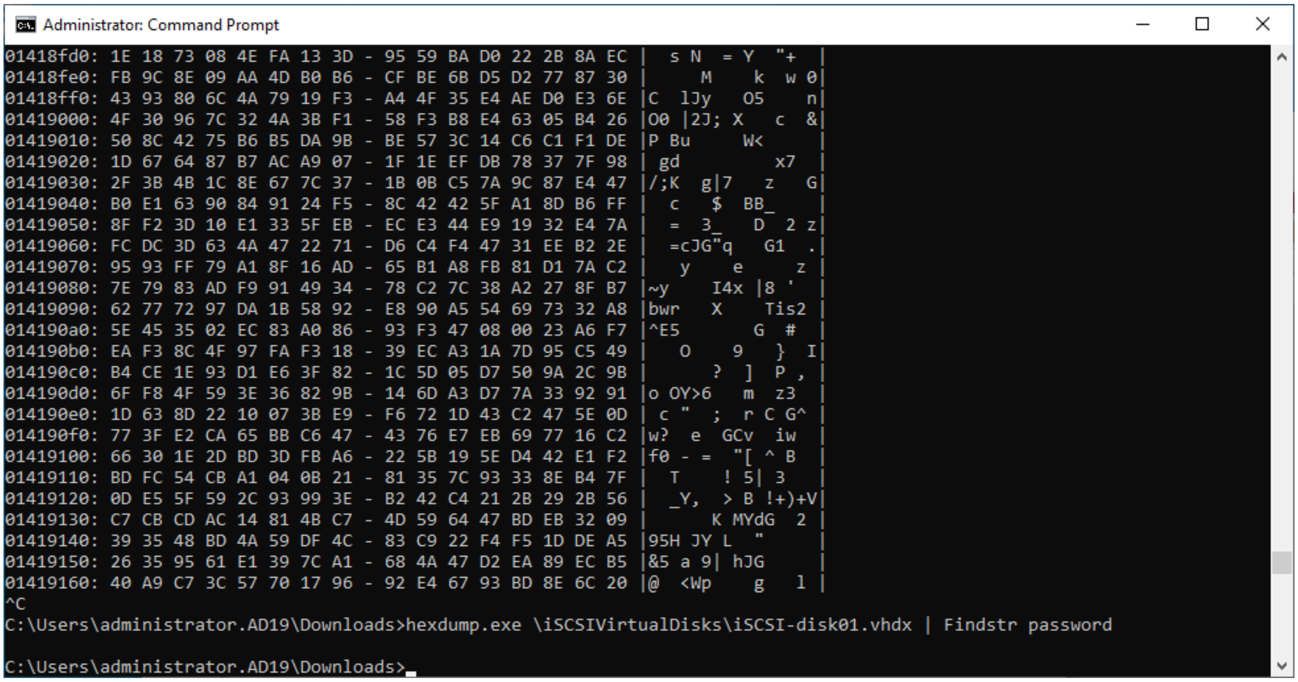


```
My IRS password: iluvyou
```

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.



```
C:\Users\administrator.AD19\Downloads>hexdump.exe \iSCSIVirtualDisks\iSCSI-disk01.vhdx
00000000: 76 68 64 78 66 69 6C 65 - 4D 00 69 00 63 00 72 00 |vhdxfileM i c r |
00000010: 6F 00 73 00 6F 00 66 00 - 74 00 20 00 57 00 69 00 |o s o f t   W i |
00000020: 6E 00 64 00 6F 00 77 00 - 73 00 20 00 31 00 30 00 |n d o w s   1 0 |
00000030: 2E 00 30 00 2E 00 32 00 - 30 00 33 00 34 00 38 00 |. 0 . 2 0 3 4 8 |
00000040: 2E 00 30 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |. 0             |
00000050: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |                |
*
00010000: 68 65 61 64 2A 71 DB FD - 0C 00 00 00 00 00 00 00 |head*q          |
00010010: 41 5E F1 A0 04 CF 84 4A - AA 33 4E 98 5B 15 1C A8 |A^     J 3N [   |
00010020: E7 E7 62 3E 18 A0 5B 40 - 9D 0A F9 B6 F2 9F FD ED |  b>  [@        |
00010030: 3A E1 8B AB F1 CE FD 48 - A6 66 B3 85 27 CD 36 7E |:      H f  ' 6~|
00010040: 00 00 01 00 00 00 10 00 - 00 00 10 00 00 00 00 00 |                |
00010050: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |                |
*
00020000: 68 65 61 64 5D ED 23 7F - 0D 00 00 00 00 00 00 00 |head] #         |
00020010: 41 5E F1 A0 04 CF 84 4A - AA 33 4E 98 5B 15 1C A8 |A^     J 3N [   |
00020020: E7 E7 62 3E 18 A0 5B 40 - 9D 0A F9 B6 F2 9F FD ED |  b>  [@        |
00020030: 3A E1 8B AB F1 CE FD 48 - A6 66 B3 85 27 CD 36 7E |:      H f  ' 6~|
00020040: 00 00 01 00 00 00 10 00 - 00 00 10 00 00 00 00 00 |                |
00020050: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |                |
*
00030000: 72 65 67 69 AE 8C 6B C6 - 02 00 00 00 00 00 00 00 |regi  k         |
00030010: 66 77 C2 2D 23 F6 00 42 - 9D 64 11 5E 9B FD 4A 08 |fw -#  B d ^  J |
00030020: 00 00 30 00 00 00 00 00 - 00 00 10 00 01 00 00 00 |  0             |
00030030: 06 A2 7C 8B 90 47 9A 4B - B8 FE 57 5F 05 0F 88 6E |  |  G K  W_   n|
00030040: 00 00 20 00 00 00 00 00 - 00 00 10 00 01 00 00 00 |                |
00030050: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |                |
*
```



```
01418fd0: 1E 18 73 08 4E FA 13 3D - 95 59 BA D0 22 2B 8A EC |  s N  = Y  "+  |
01418fe0: FB 9C 8E 09 AA 4D B0 B6 - CF BE 6B D5 D2 77 87 30 |     M    k  w 0|
01418ff0: 43 93 80 6C 4A 79 19 F3 - A4 4F 35 E4 AE D0 E3 6E |C  lJy   O5    n|
01419000: 4F 30 96 7C 32 4A 3B F1 - 58 F3 B8 E4 63 05 B4 26 |O0 |2J; X   c  &|
01419010: 50 8C 42 75 B6 B5 DA 9B - BE 57 3C 14 C6 C1 F1 DE |P Bu     W<     |
01419020: 1D 67 64 87 B7 AC A9 07 - 1F 1E EF DB 78 37 7F 98 | gd         x7  |
01419030: 2F 3B 4B 1C 8E 67 7C 37 - 1B 0B C5 7A 9C 87 E4 47 |/;K  g|7   z   G|
01419040: B0 E1 63 90 84 91 24 F5 - 8C 42 42 5F A1 8D B6 FF |  c   $  BB_     |
01419050: 8F F2 3D 10 E1 33 5F EB - EC E3 44 E9 19 32 E4 7A |  =  3_   D  2 z|
01419060: FC DC 3D 63 4A 47 22 71 - D6 C4 F4 47 31 EE B2 2E |  =cJG"q   G1  .|
01419070: 95 93 FF 79 A1 8F 16 AD - 65 B1 A8 FB 81 D1 7A C2 |   y    e     z |
01419080: 7E 79 83 AD F9 91 49 34 - 78 C2 7C 38 A2 27 8F B7 |~y     I4x |8 ' |
01419090: 62 77 72 97 DA 1B 58 92 - E8 90 A5 54 69 73 32 A8 |bwr   X    Tis2 |
014190a0: 5E 45 35 02 EC 83 A0 86 - 93 F3 47 08 00 23 A6 F7 |^E5        G  # |
014190b0: EA F3 8C 4F 97 FA F3 18 - 39 EC A3 1A 7D 95 C5 49 |   O    9   }  I|
014190c0: B4 CE 1E 93 D1 E6 3F 82 - 1C 5D 05 D7 50 9A 2C 9B |      ?  ]  P , |
014190d0: 6F F8 4F 59 3E 36 82 9B - 14 6D A3 D7 7A 33 92 91 |o OY>6   m  z3  |
014190e0: 1D 63 8D 22 10 07 3B E9 - F6 72 1D 43 C2 47 5E 0D | c "  ;  r C G^ |
014190f0: 77 3F E2 CA 65 BB C6 47 - 43 76 E7 EB 69 77 16 C2 |w?  e  GCv  iw  |
01419100: 66 30 1E 2D BD 3D FB A6 - 22 5B 19 5E D4 42 E1 F2 |f0 - =  "[ ^ B  |
01419110: BD FC 54 CB A1 04 0B 21 - 81 35 7C 93 33 8E B4 7F |  T    ! 5| 3   |
01419120: 0D E5 5F 59 2C 93 99 3E - B2 42 C4 21 2B 29 2B 56 |  _Y,  > B !+)+V|
01419130: C7 CB CD AC 14 81 4B C7 - 4D 59 64 47 BD EB 32 09 |      K MYdG  2 |
01419140: 39 35 48 BD 4A 59 DF 4C - 83 C9 22 F4 F5 1D DE A5 |95H JY L  "     |
01419150: 26 35 95 61 E1 39 7C A1 - 68 4A 47 D2 EA 89 EC B5 |&5 a 9| hJG     |
01419160: 40 A9 C7 3C 57 70 17 96 - 92 E4 67 93 BD 8E 6C 20 |@  <Wp    g   l |
^C
C:\Users\administrator.AD19\Downloads>hexdump.exe \iSCSIVirtualDisks\iSCSI-disk01.vhdx | Findstr password

C:\Users\administrator.AD19\Downloads>
```

Conclusion

In this integration guide, we have shown how to set up Bloombase StoreSafe Intelligent Storage Firewall with HashiCorp Vault to deliver on-the-fly encryption of multiple storage protocols including SMB, NFS and iSCSI. The end result is a high-bandwidth, application-transparent storage encryption solution with centralized key management 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,

- HashiCorp Vault

has been integrated with Bloombase StoreSafe Intelligent Storage Firewall to deliver encryption security of Microsoft Storage Server on Microsoft Windows Server 2022 over SMB/CIFS, NFS and iSCSI network storage protocols for software applications running on Microsoft Windows Server 2022 and Windows 11.

Bloombase Product	Application Components	Key Manager
Bloombase StoreSafe Intelligent Storage Firewall	• Microsoft Storage Server • Microsoft Windows Server 2022 • Microsoft Windows 11	• HashiCorp Vault 1.8.3+ent

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 HashiCorp team for supporting the integration of Bloombase StoreSafe with HashiCorp Vault.

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. HashiCorp Vault, https://www.vaultproject.io/
4. HashiCorp Vault Enterprise, https://www.hashicorp.com/products/vault
5. OASIS KMIP, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip