interopLab

Interoperability of Bloombase StoreSafe and Thales Vormetric Data Security Manager (DSM) for On-premises Traditional Data Center and Off-premises Cloud Data-at-Rest Encryption

November 2018

BLOOMBASE®

Executive Summary

Thales Vormetric Data Security Manager (DSM) is validated by Bloombase InteropLab to run with Bloombase StoreSafe data-at-rest encryption security solution. This document describes the steps carried out to test interoperability of Thales Vormetric Data Security Manager (DSM) with Bloombase StoreSafe software appliance on Intel-based hardware server. Client host systems on Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Oracle Sun Solaris, IBM AIX and HP-UX are tested with Bloombase StoreSafe and Thales Vormetric Data Security Manager (DSM) securing on-premises HPE MSA P2000 storage system, Microsoft Windows Storage Server on Microsoft Windows Server 2019 and off-premises Amazon cloud storage services.

Document No.: BLBS-TN-Bloombase-StoreSafe-Thales-Vormetric-Data-Security-Manager-DSM-Interoperability-USLET-EN-R0.93

Table of Contents

Purpose and Scope

This document describes the steps necessary to integrate Thales Vormetric Data Security Manager (DSM) with Bloombase StoreSafe to secure sensitive enterprise business data-at-rest managed in storage systems and cloud storage services. Specifically, we cover the following topics:

- Install and configure Bloombase StoreSafe
- Integrate Bloombase StoreSafe with Thales Vormetric Data Security Manager (DSM)
- Interoperability testing on client host systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris with storage backends including Microsoft Windows Storage Server, HPE MSA disk array and Amazon cloud storage services

Assumptions

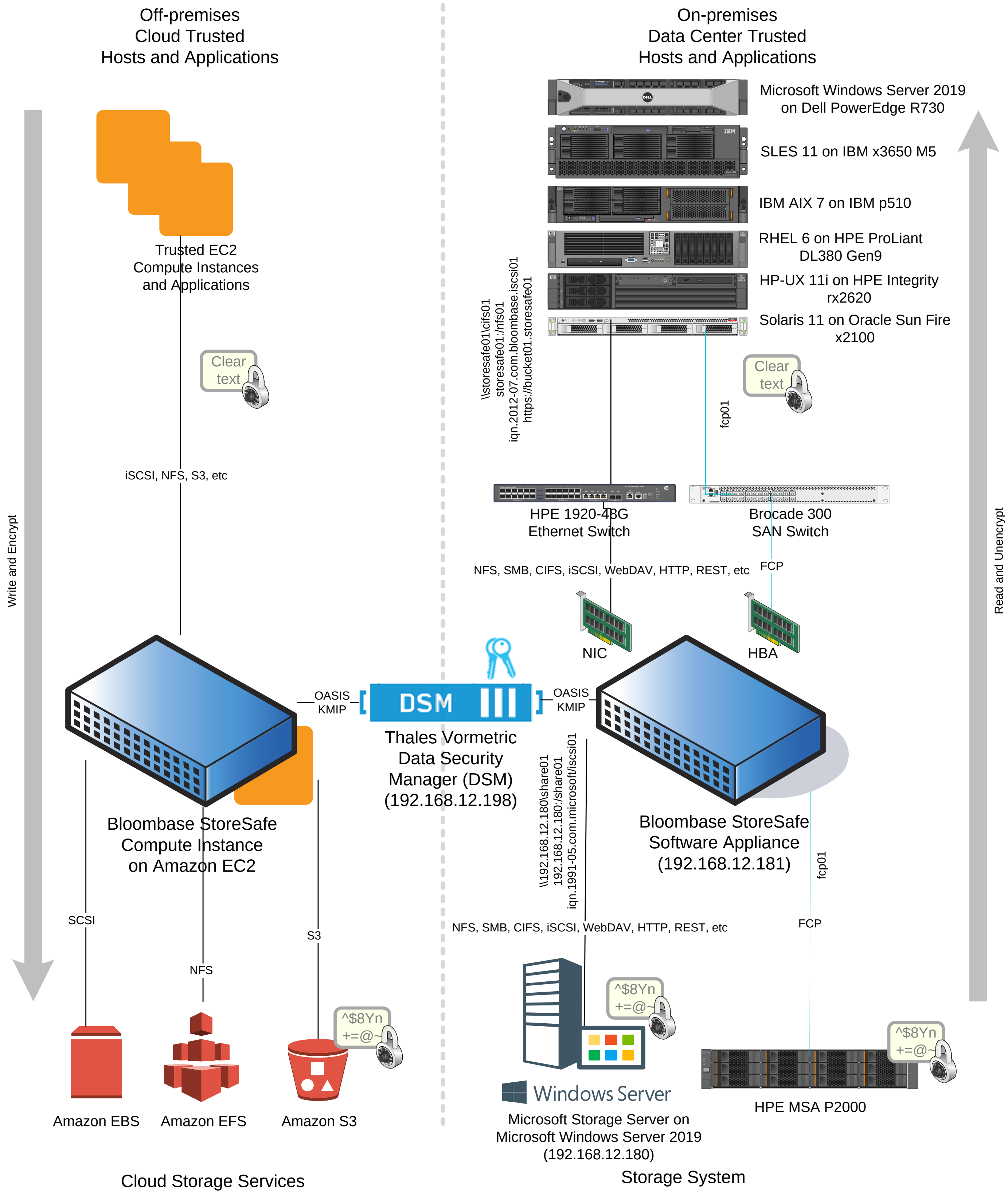
This document describes interoperability testing of Thales Vormetric Data Security Manager (DSM) with Bloombase StoreSafe. Therefore, it is assumed that the reader is familiar with operation of Thales Vormetric Data Security Manager (DSM), storage systems and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is also assumed that the reader possesses basic UNIX administration skill-set. The examples provided may require modifications before they could be run in reader's IT environment.

As Thales Vormetric Data Security Manager (DSM) is a third-party option to Bloombase StoreSafe data-at-rest encryption security solution, the reader is recommended to refer to installation and configuration guides of specific model of Thales Vormetric Data Security Manager (DSM) for the actual use case. We assume the reader has 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 validation testing environment is set up as in below diagram:


Off-premises
Cloud Trusted
Hosts and Applications
On-premises
Data Center Trusted
Hosts and Applications
Trusted EC2
Compute Instances
and Applications
Clear
text
iSCSI, NFS, S3, etc
Write and Encrypt
Microsoft Windows Server 2019
on Dell PowerEdge R730
SLES 11 on IBM x3650 M5
IBM AIX 7 on IBM p510
RHEL 6 on HPE ProLiant
DL380 Gen9
HP-UX 11i on HPE Integrity
rx2620
Solaris 11 on Oracle Sun Fire
x2100
\\storesafe01\cifs01
storesafe01:/nfs01
iqn.2012-07.com.bloombase.iscsi01
https://bucket01.storesafe01
Clear
text
fcp01
HPE 1920-48G
Ethernet Switch
Brocade 300
SAN Switch
NFS, SMB, CIFS, iSCSI, WebDAV, HTTP, REST, etc
FCP
NIC
HBA
Read and Unencrypt
OASIS
KMIP
DSM
Thales Vormetric
Data Security
Manager (DSM)
(192.168.12.198)
OASIS
KMIP
Bloombase StoreSafe
Compute Instance
on Amazon EC2
Bloombase StoreSafe
Software Appliance
(192.168.12.181)
\\192.168.12.180\share01
192.168.12.180:/share01
iqn.1991-05.com.microsoft/iscsi01
fcp01
SCSI
NFS
S3
NFS, SMB, CIFS, iSCSI, WebDAV, HTTP, REST, etc
FCP
^$8Yn
+=@~
^$8Yn
+=@~
^$8Yn
+=@~
Amazon EBS
Amazon EFS
Amazon S3
Windows Server
Microsoft Storage Server on
Microsoft Windows Server 2019
(192.168.12.180)
HPE MSA P2000
Cloud Storage Services
Storage System

Key Management System

Key Management System	Thales Vormetric Data Security Manager (DSM)

On-premises Data-at-Rest Encryption

Bloombase StoreSafe	Bloombase StoreSafe Software Appliance v3.4.7
Hypervisor	VMware ESXi 6.0
Server	HPE ProLiant DL320e
Processor	1x Intel Xeon E3-1220 v3 with AES-NI
Memory	8 GB
Network Interface Card	On-board HPE 1GbE NIC
Host Bus Adapter	Cavium QLogic QLE2672 16G FC HBA

Off-premises Data-at-Rest Encryption

Bloombase StoreSafe	Bloombase StoreSafe Compute Instance v3.4.7 on Amazon EC2
Cloud Platform	Amazon EC2
Processor	4x vCPU
Memory	8 GB
Network Interface Card	Amazon Virtual NIC

On-premises Storage

Storage Systems	• Microsoft Windows Storage Server on Microsoft Windows Server 2019 • HPE MSA P2000 Disk Array System

Off-premises Storage

Cloud Storage Services	• Amazon Simple Storage Service (S3) • Amazon Elastic Block Store (EBS) • Amazon Elastic File System (EFS)

Client Hosts

Model	Dell PowerEdge R730	HPE ProLiant DL380 Gen9	Lenovo System x3650 M5	HPE Integrity rx2620	IBM System p5 510	Oracle Sun Fire x2100
Operating System	Microsoft Windows Server 2019	Red Hat Enterprise Linux 6	SUSE Linux Enterprise 11	HP-UX 11i	IBM AIX 7	Oracle Solaris 11

Configuration Overview

Thales Vormetric Data Security Manager (DSM)

Thales Vormetric Data Security Manager (DSM) enables centralized management of key management, simplifying deployment and operations. The DSM is available in different form factors and FIPS 140-2 levels. Customers may deploy virtual appliances on-premises, in private and public clouds or select high-assurance hardware to meet their key management and security requirements.

The DSM is offered as a FIPS 140-2 Level 1 virtual appliance, as well as two hardware appliances: the V6000, which is FIPS 140-2 Level 2 certified, and the V6100, which is FIPS 140-2 Level 3 certified. The platform is available on the Amazon Web Services (AWS) Marketplace and the Microsoft Azure Marketplace.

The DSM provides central management and secure storage of encryption keys, including those generated by Thales e-Security product, and KMIP-compliant third-party products. It provides intuitive web-based console, CLI, and APIs for managing of encryption keys.

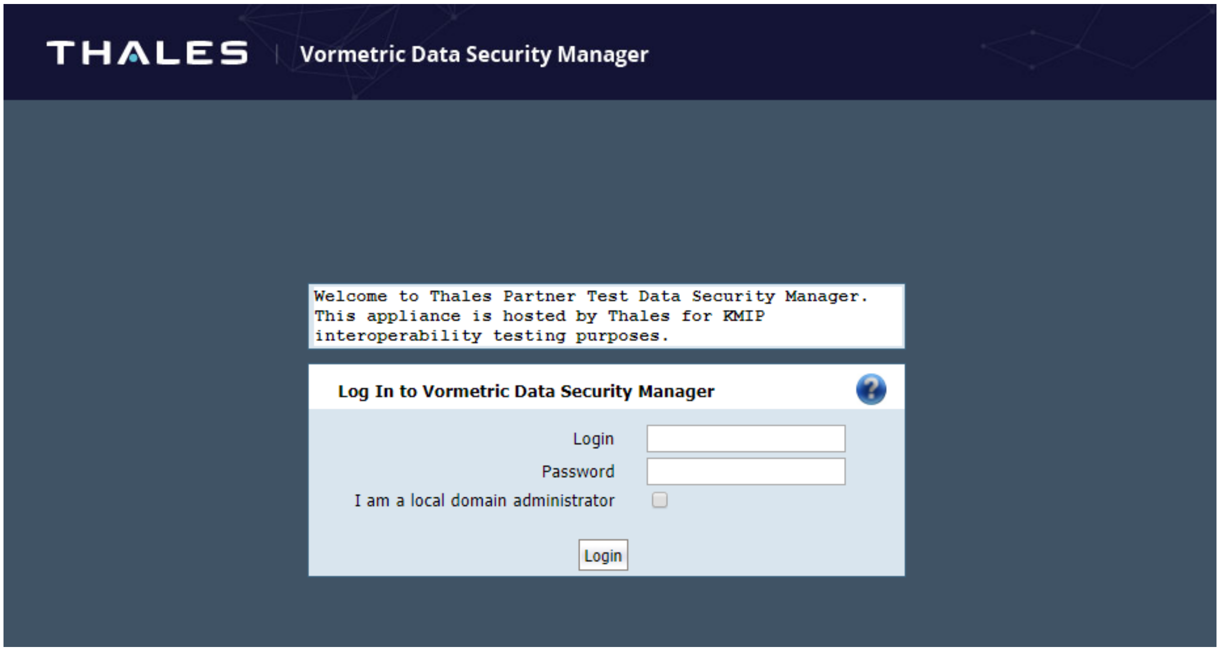
To maximize uptime and security, the DSM features redundant components and the ability to cluster appliances for fault tolerance and high availability. Strong separation-of-duties polices can be enforced to ensure that one administrator does not have complete control over encryption keys or administration. In addition, the DSM supports two-factor authentication for administrative access as well as Thales nShield Remote Administration with smart card access in the V6100.

The KMIP services provided by Thales Vormetric Data Security Manager (DSM) are used by Bloombase StoreSafe for encryption protection of data-at-rest use cases.

Thales Vormetric Data Security Manager (DSM) Configurations

Assume Thales Vormetric Data Security Manager (DSM) is installed and configured as a network attached appliance with IP address `192.168.12.198`.

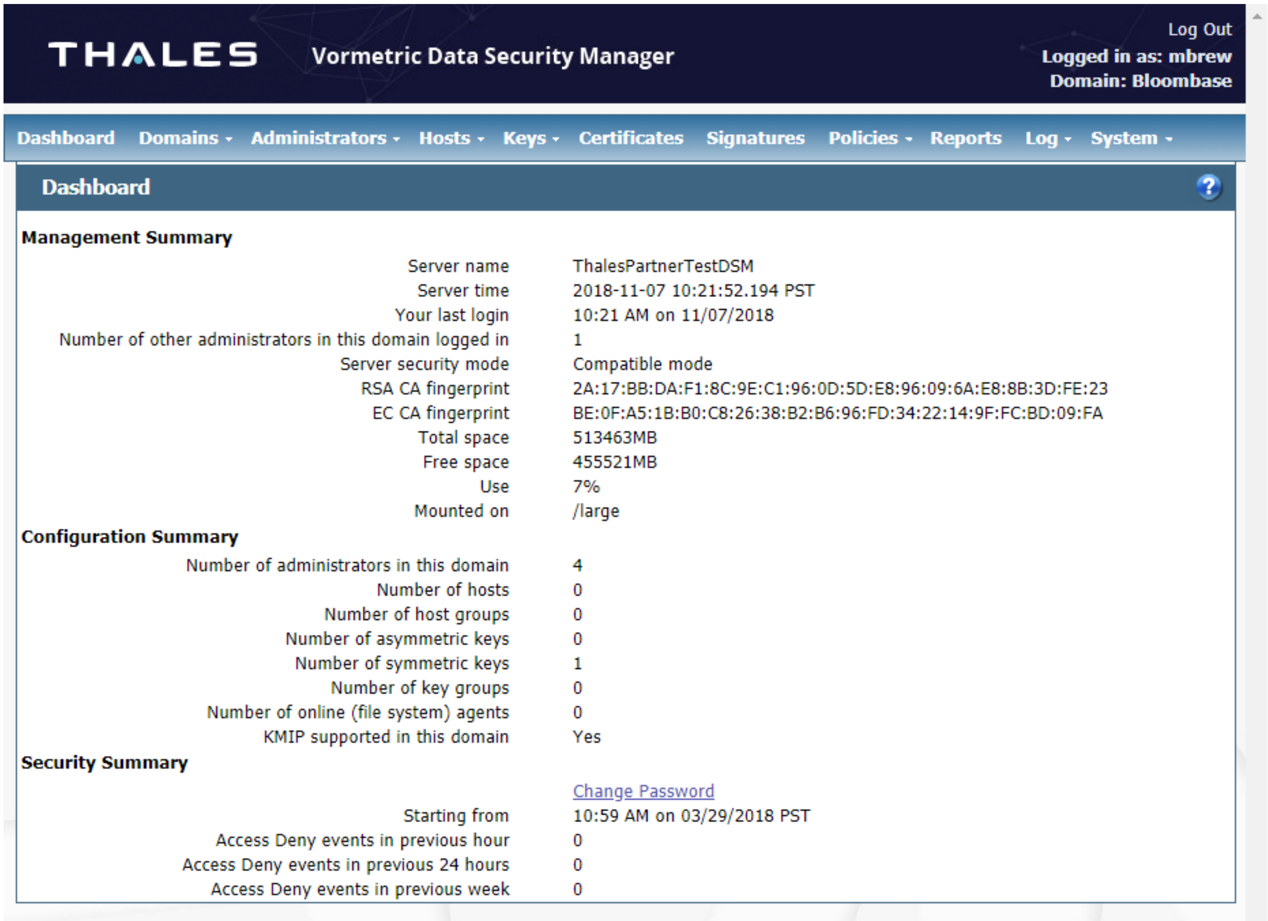
Thales Vormetric Data Security Manager (DSM) can be managed remotely via web-based management console at URL `https://192.168.12.198:8445`.



Welcome to Thales Partner Test Data Security Manager. This appliance is hosted by Thales for KMIP interoperability testing purposes.

THALES
Vormetric Data Security Manager
Log In to Vormetric Data Security Manager
Login
Password
I am a local domain administrator
Login

Once logged in, the dashboard of the Thales Vormetric Data Security Manager (DSM) is shown.



Dashboard

Management Summary

Server name	ThalesPartnerTestDSM
Server time	2018-11-07 10:21:52.194 PST
Your last login	10:21 AM on 11/07/2018
Number of other administrators in this domain logged in	1
Server security mode	Compatible mode
RSA CA fingerprint	2A:17:BB:DA:F1:8C:9E:C1:96:0D:5D:E8:96:09:6A:E8:8B:3D:FE:23
EC CA fingerprint	BE:0F:A5:1B:B0:C8:26:38:B2:B6:96:FD:34:22:14:9F:FC:BD:09:FA
Total space	513463MB
Free space	455521MB
Use	7%
Mounted on	/large

Configuration Summary

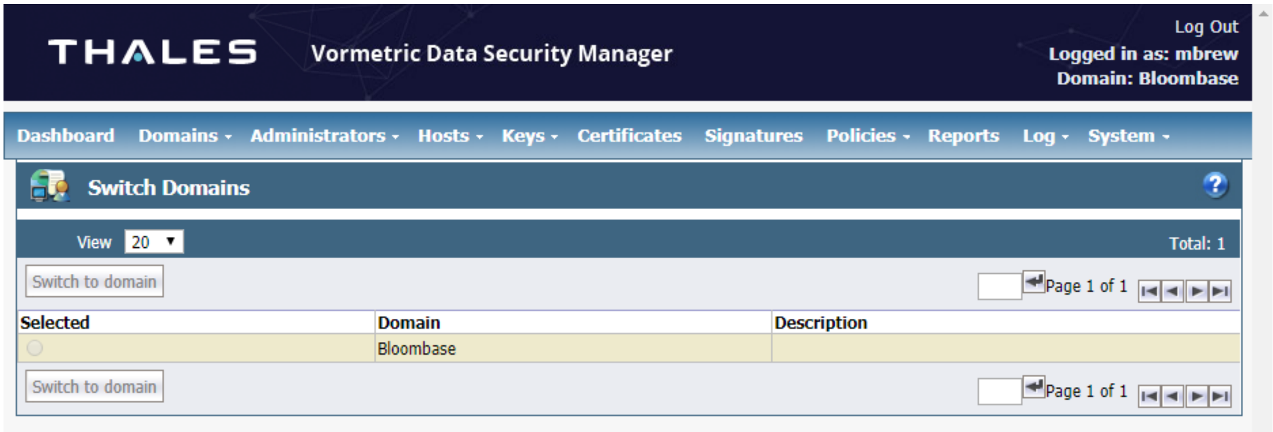
Number of administrators in this domain	4
Number of hosts	0
Number of host groups	0
Number of asymmetric keys	0
Number of symmetric keys	1
Number of key groups	0
Number of online (file system) agents	0
KMIP supported in this domain	Yes

Security Summary

	Change Password
Starting from	10:59 AM on 03/29/2018 PST
Access Deny events in previous hour	0
Access Deny events in previous 24 hours	0
Access Deny events in previous week	0

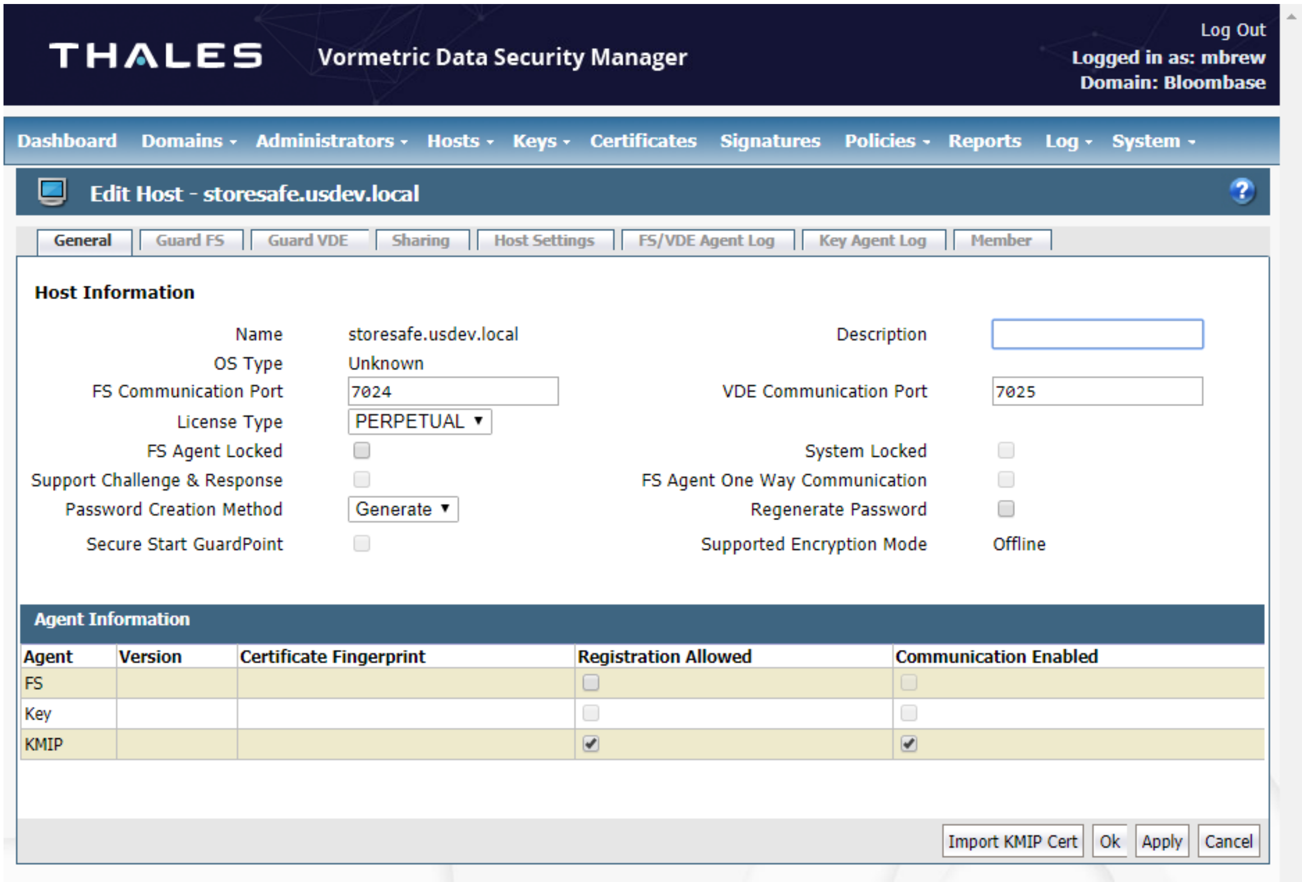
To authenticate the communication between Thales Vormetric Data Security Manager (DSM) and Bloombase StoreSafe, signed certificates need to be created and stored in the Thales Vormetric Data Security Manager (DSM) and the Bloombase StoreSafe. In the Thales Vormetric Data Security Manager (DSM), this can be configured as follows.

Select the domain to be configured, in this case, `Bloombase`.



Selected	Domain	Description
○	Bloombase	

Provision the authorized agent host which key management services are to be delivered, in this case, the Bloombase StoreSafe server instance namely `storesafe.usdev.local`



Edit Host - storesafe.usdev.local

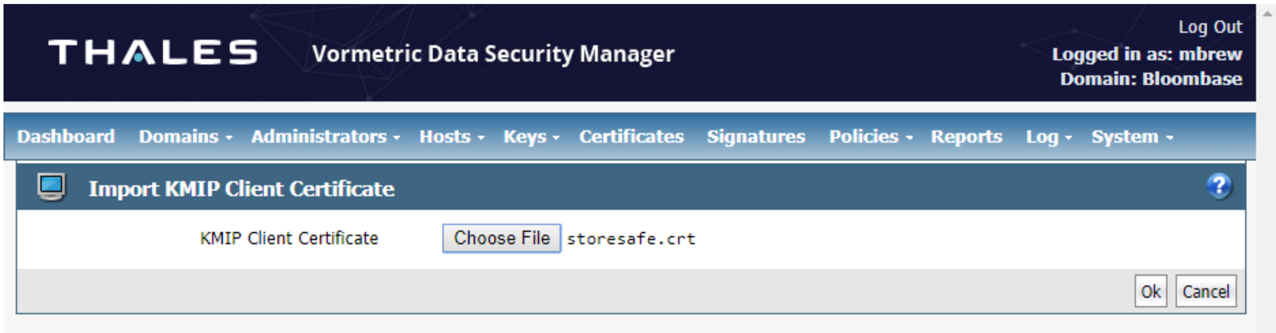
Host Information

Name	storesafe.usdev.local	Description	
OS Type	Unknown		
FS Communication Port	7024	VDE Communication Port	7025
License Type	PERPETUAL		
FS Agent Locked	□	System Locked	□
Support Challenge & Response	□	FS Agent One Way Communication	□
Password Creation Method	Generate	Regenerate Password	□
Secure Start GuardPoint	□	Supported Encryption Mode	Offline

Agent Information

Agent	Version	Certificate Fingerprint	Registration Allowed	Communication Enabled
FS			□	□
Key			□	□
KMIP			☑	☑

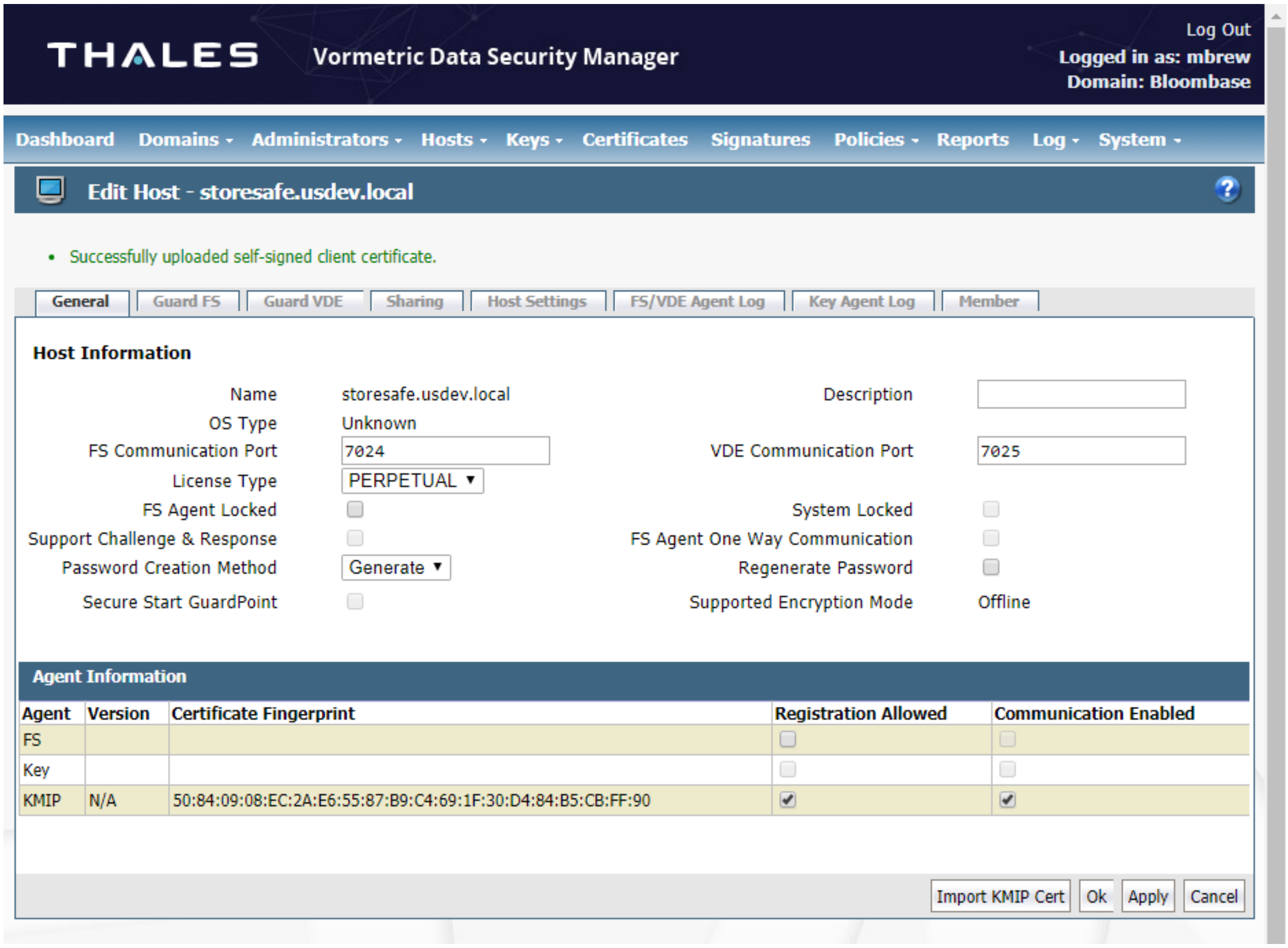
KMIP service is provisioned for the trusted host, in this case, the Bloombase StoreSafe server instance namely `storesafe.usdev.local`



Import KMIP Client Certificate

KMIP Client Certificate: storesafe.crt

KMIP client certificate is generated and imported to DSM host configuration.



Edit Host - storesafe.usdev.local

- Successfully uploaded self-signed client certificate.

Host Information

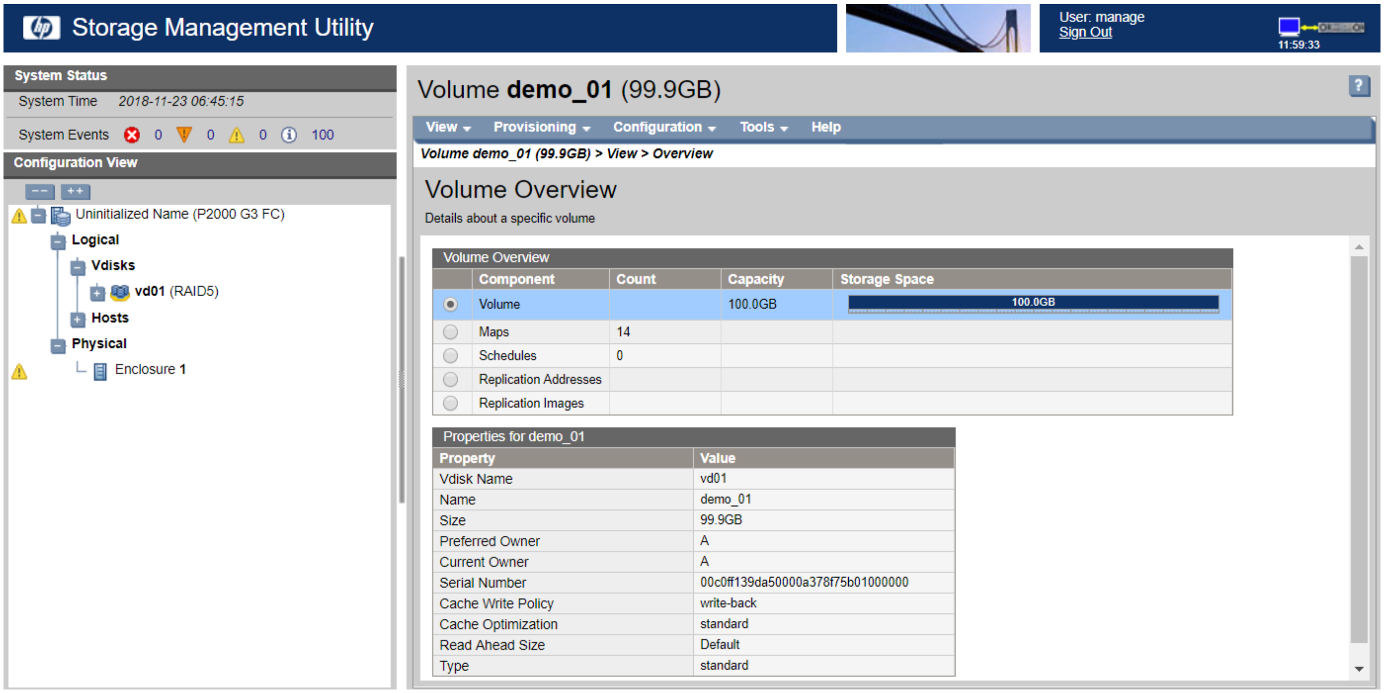
Name	storesafe.usdev.local	Description	
OS Type	Unknown		
FS Communication Port	7024	VDE Communication Port	7025
License Type	PERPETUAL		
FS Agent Locked	☐	System Locked	☐
Support Challenge & Response	☐	FS Agent One Way Communication	☐
Password Creation Method	Generate	Regenerate Password	☐
Secure Start GuardPoint	☐	Supported Encryption Mode	Offline

Agent Information

Agent	Version	Certificate Fingerprint	Registration Allowed	Communication Enabled
FS			☐	☐
Key			☐	☐
KMIP	N/A	50:84:09:08:EC:2A:E6:55:87:B9:C4:69:1F:30:D4:84:B5:CB:FF:90	☑	☑

HPE P2000 G3 MSA Disk Array Storage System

The HPE P2000 G3 MSA Disk Array Storage System used in this interoperability test is a storage area network (SAN) disk array capable of providing FCP network storage protocol.



System Time 2018-11-23 06:45:15

System Events 0 0 0 100

Volume **demo_01** (99.9GB)

Volume demo_01 (99.9GB) > View > Overview

Volume Overview

Details about a specific volume

Volume Overview

	Component	Count	Capacity	Storage Space
●	Volume		100.0GB	100.0GB
○	Maps	14		
○	Schedules	0		
○	Replication Addresses			
○	Replication Images			

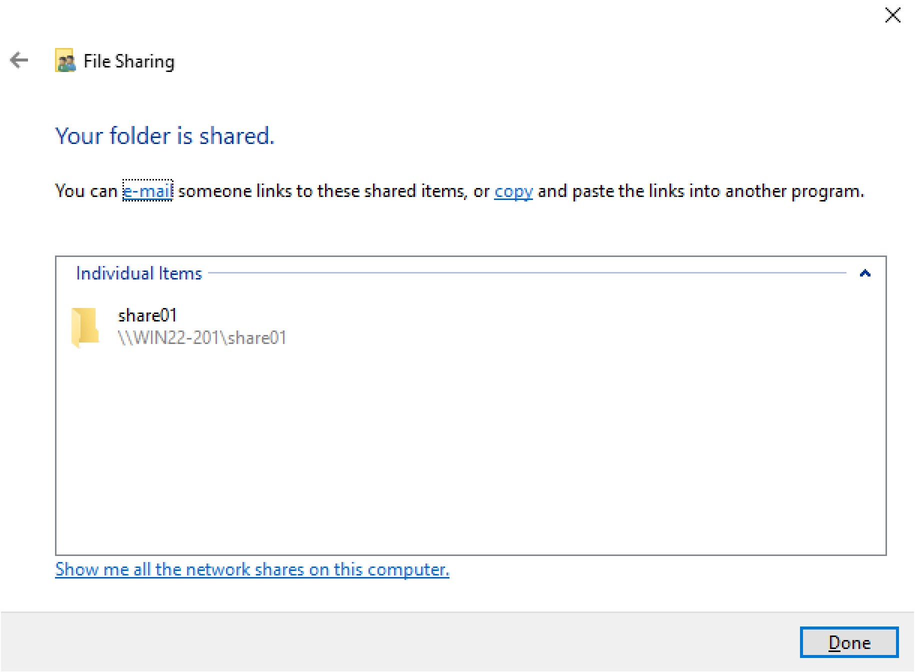
Properties for demo_01

Property	Value
Vdisk Name	vd01
Name	demo_01
Size	99.9GB
Preferred Owner	A
Current Owner	A
Serial Number	00c0ff139da50000a378f75b01000000
Cache Write Policy	write-back
Cache Optimization	standard
Read Ahead Size	Default
Type	standard

FCP block-based storage resources are provisioned on HPE P2000 G3 MSA disk array for FCP test cases in this interoperability testing.

Microsoft Windows Stroage Server on Microsoft Windows Server 2019

A Microsoft Windows Server 2019 file share namely `share01` is created as the storage backend used in this interoperability test effort.



Your folder is shared.

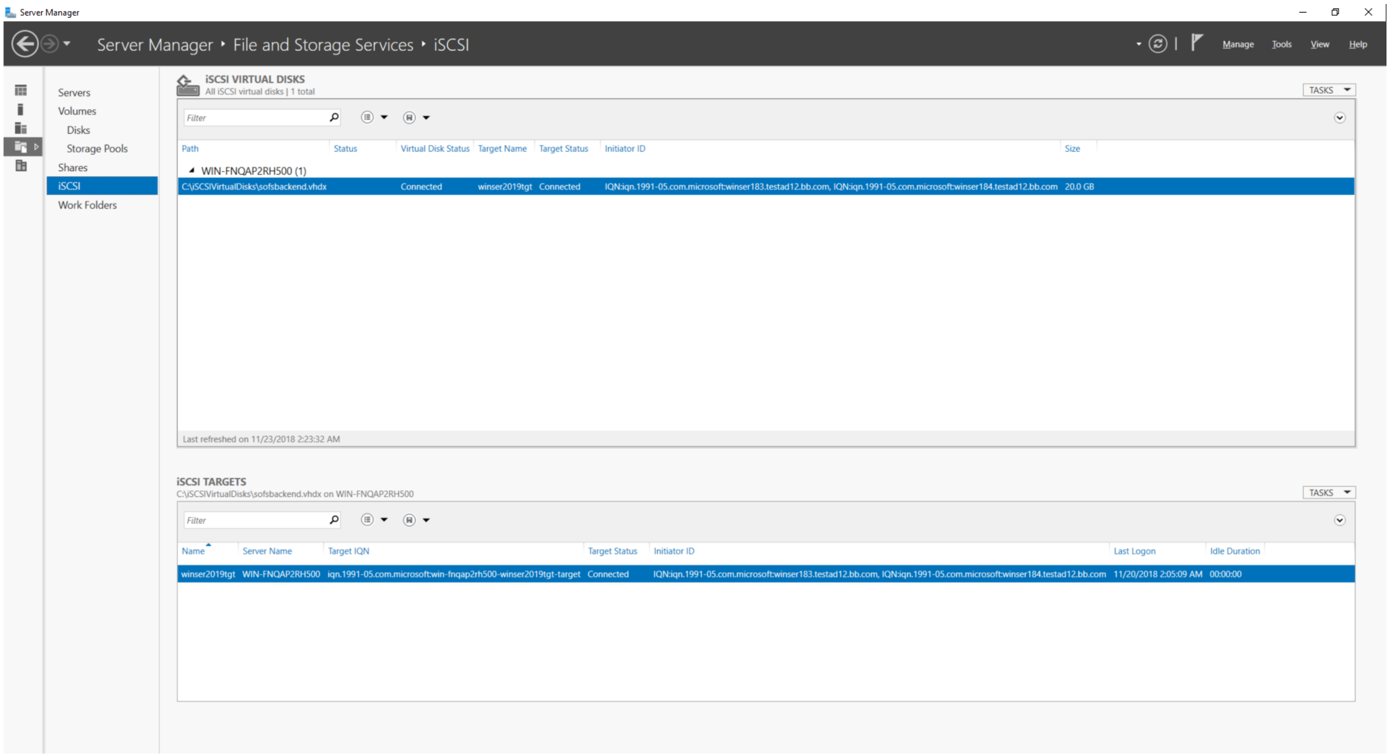
You can e-mail someone links to these shared items, or copy and paste the links into another program.

Individual Items

share01
\\WIN22-201\share01

Show me all the network shares on this computer.

Additionally, iSCSI block-based storage resources are provisioned on the Microsoft Windows Server 2019 for iSCSI test cases in this interoperability testing.



iSCSI VIRTUAL DISKS
All iSCSI virtual disks | 1 total

Path	Status	Virtual Disk Status	Target Name	Target Status	Initiator ID	Size
WIN-FNQAP2RH500 (1)						
C:\iSCSIVirtualDisks\sofsbackend.vhdx		Connected	winser2019tgt	Connected	IQN:iqn.1991-05.com.microsoft:winser183.testad12.bb.com, IQN:iqn.1991-05.com.microsoft:winser184.testad12.bb.com	20.0 GB

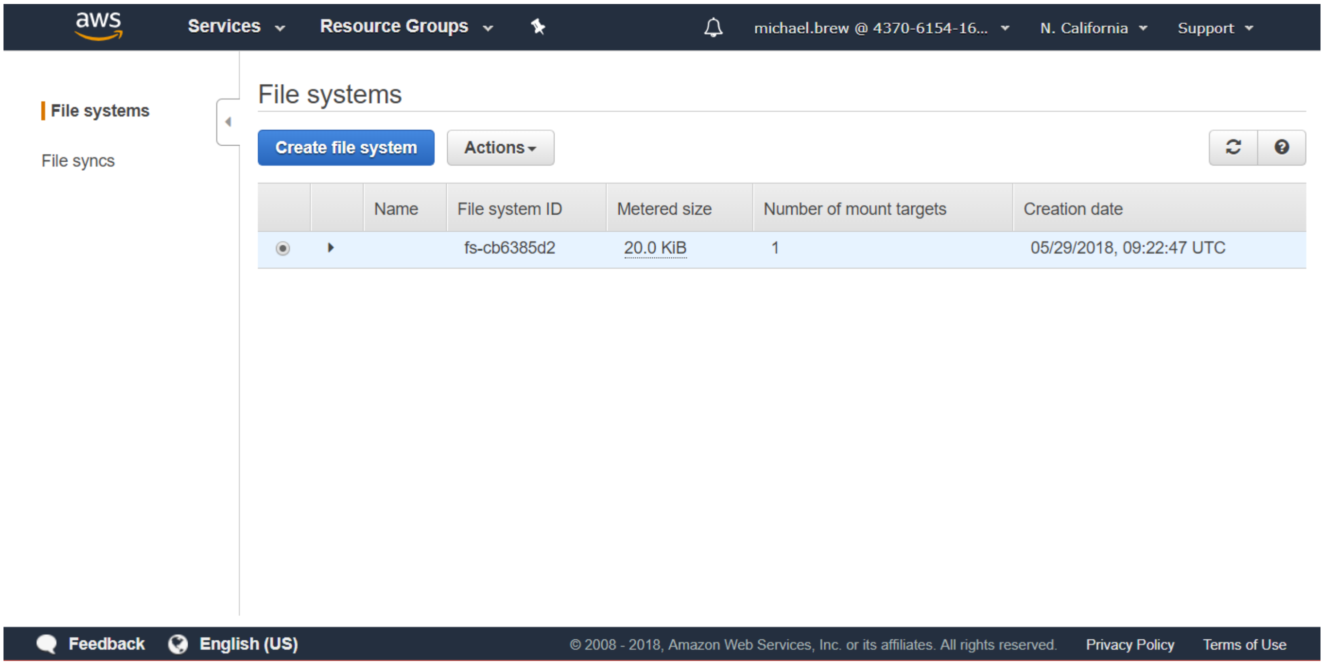
Last refreshed on 11/23/2018 2:23:32 AM

iSCSI TARGETS
C:\iSCSIVirtualDisks\sofsbackend.vhdx on WIN-FNQAP2RH500

Name	Server Name	Target IQN	Target Status	Initiator ID	Last Logon	Idle Duration
winser2019tgt	WIN-FNQAP2RH500	iqn.1991-05.com.microsoft:win-fnqap2rh500-winser2019tgt-target	Connected	IQN:iqn.1991-05.com.microsoft:winser183.testad12.bb.com, IQN:iqn.1991-05.com.microsoft:winser184.testad12.bb.com	11/20/2018 2:05:09 AM	00:00:00

Amazon EFS Cloud Storage Services

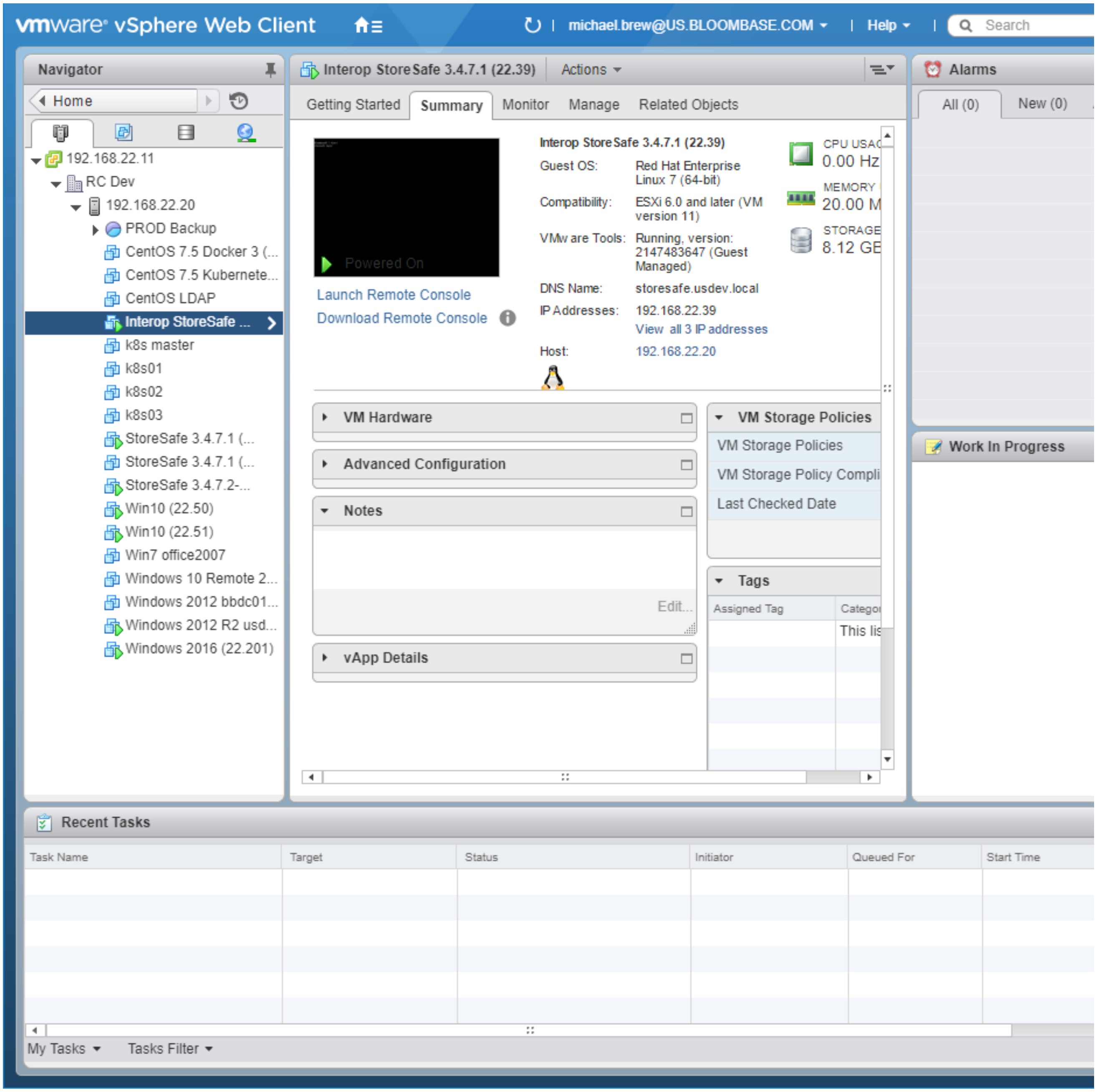
NFS file-based storage resources are provisioned on Amazon EFS for NFS test cases in this interoperability testing.



		Name	File system ID	Metered size	Number of mount targets	Creation date
●	▸		fs-cb6385d2	20.0 KiB	1	05/29/2018, 09:22:47 UTC

Bloombase StoreSafe

Bloombase StoreSafe delivers unified data-at-rest encryption security of block storage volumes, files, objects, sequential storage devices, etc. In this interoperability test, file-based encryption security service is validated against Bloombase StoreSafe with keys managed at Thales Vormetric Data Security Manager (DSM).



Interop StoreSafe 3.4.7.1 (22.39)

Guest OS: Red Hat Enterprise Linux 7 (64-bit)

Compatibility: ESXi 6.0 and later (VM version 11)

VMware Tools: Running, version: 2147483647 (Guest Managed)

DNS Name: storesafe.usdev.local

IP Addresses: 192.168.22.39

View all 3 IP addresses

Host: 192.168.22.20

CPU USAG 0.00 Hz

MEMORY 20.00 M

STORAGE 8.12 GE

Bloombase StoreSafe software appliance is deployed as virtual appliance (VA) on VMware ESXi and as compute instance on Amazon EC2.

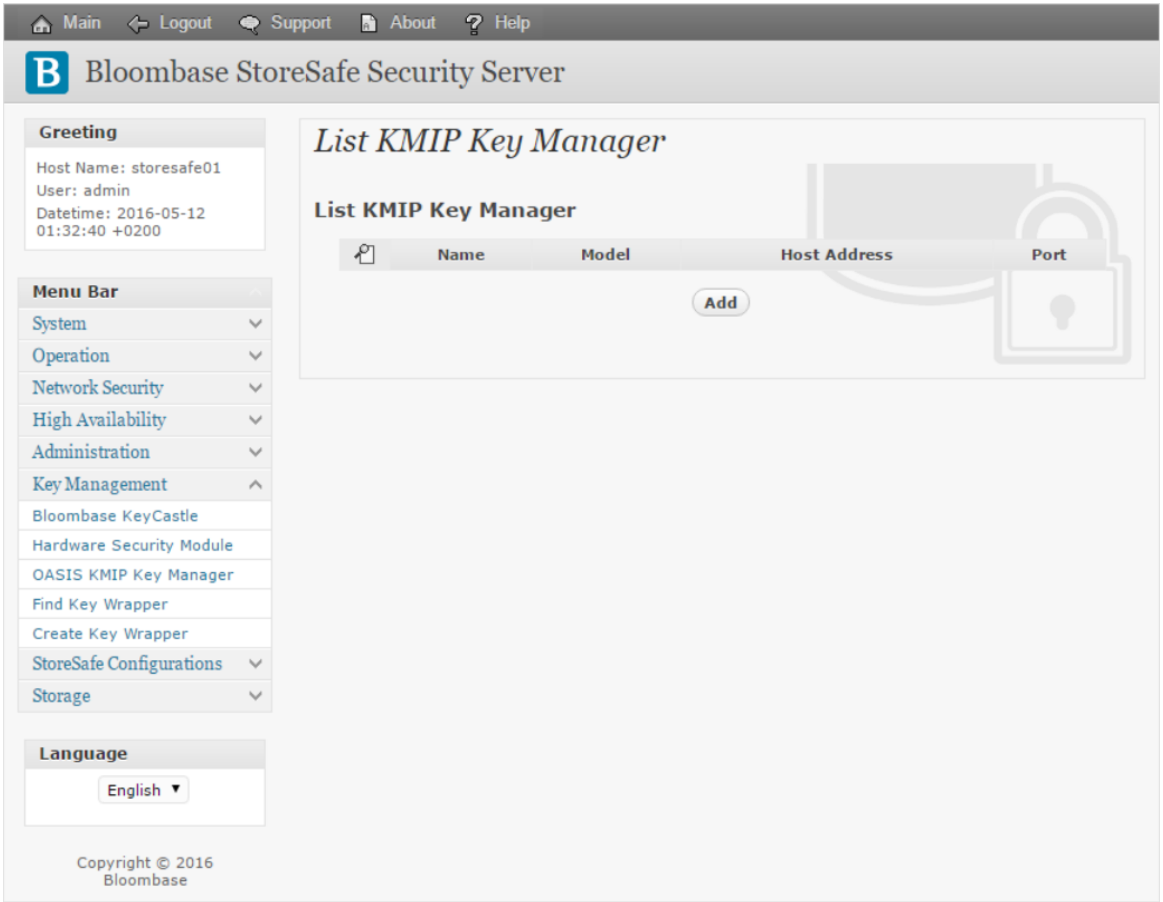
Network Security, Trust and Authentication Configuration

In this interoperability test effort, Bloombase StoreSafe serves as the user of Thales Vormetric Data Security Manager (DSM) for encryption key access to deliver data at-rest encryption services. Authentication of Bloombase StoreSafe to the Thales Vormetric Data Security Manager (DSM) can be achieved with signed certificates through SSL communications.

Thales Vormetric Data Security Manager (DSM) and Bloombase KeyCastle Integration

Bloombase supports Thales Vormetric Data Security Manager (DSM) 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 Thales Vormetric Data Security Manager (DSM), the KMIP service configuration at Bloombase web management console has to be set up. This is done by clicking “OASIS KMIP Key Manager” under “Key Management”.

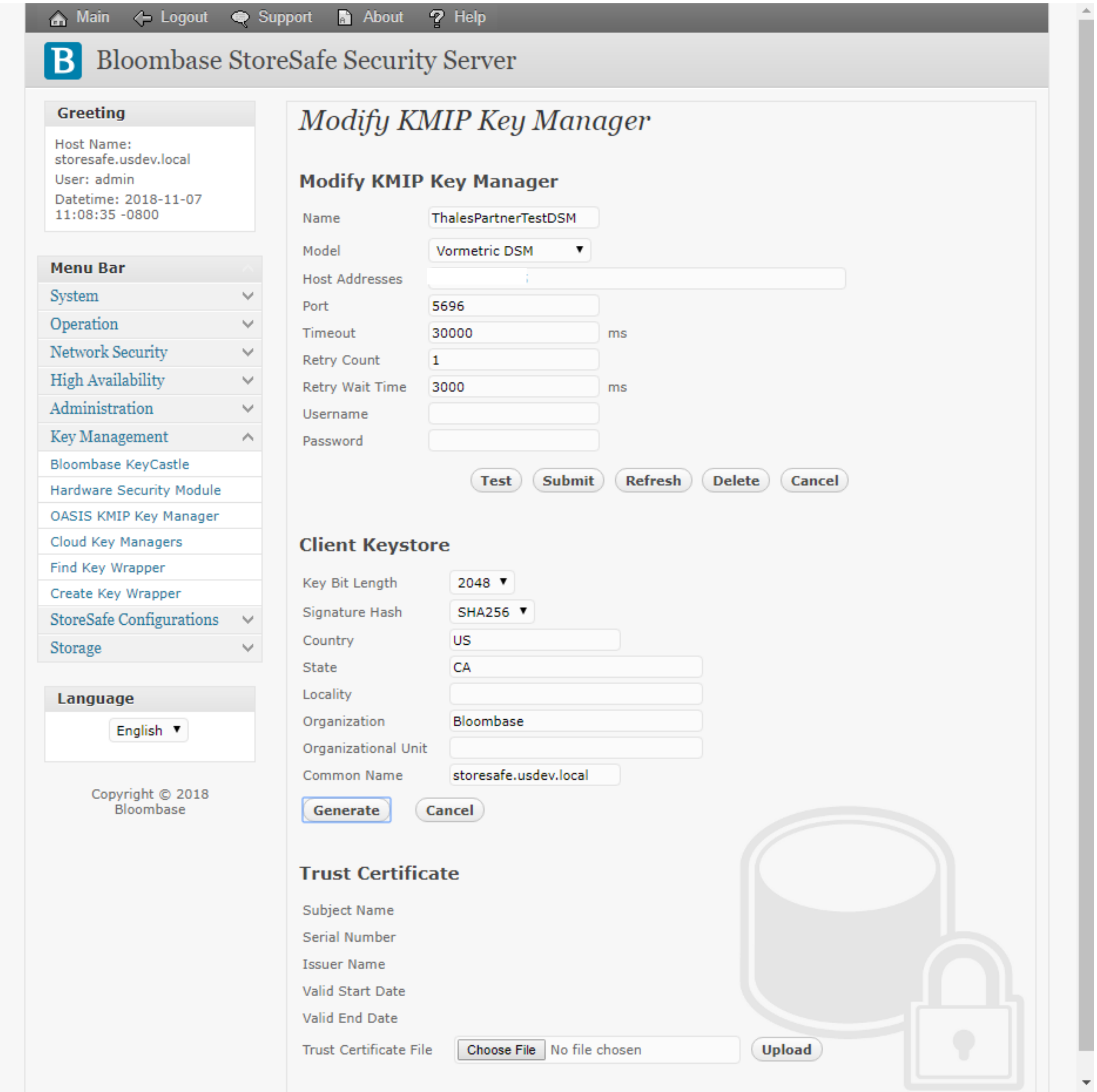


Host Name: storesafe01
User: admin
Datetime: 2016-05-12 01:32:40 +0200

List KMIP Key Manager

	Name	Model	Host Address	Port

Input a name for the Thales Vormetric Data Security Manager (DSM), and select Model as `Vormetric DSM`. Input also the host address and port to access the Thales Vormetric Data Security Manager (DSM), and import the signed X.509 key pair as "Client Keystore", the certificate of the local root CA on Thales Vormetric Data Security Manager (DSM) as "Trust Certificate".



Greeting

Host Name: storesafe.usdev.local
User: admin
Datetime: 2018-11-07 11:08:35 -0800

Copyright © 2018 Bloombase

Modify KMIP Key Manager

Modify KMIP Key Manager

Name	ThalesPartnerTestDSM
Model	Vormetric DSM
Host Addresses	
Port	5696
Timeout	30000 ms
Retry Count	1
Retry Wait Time	3000 ms
Username	
Password	

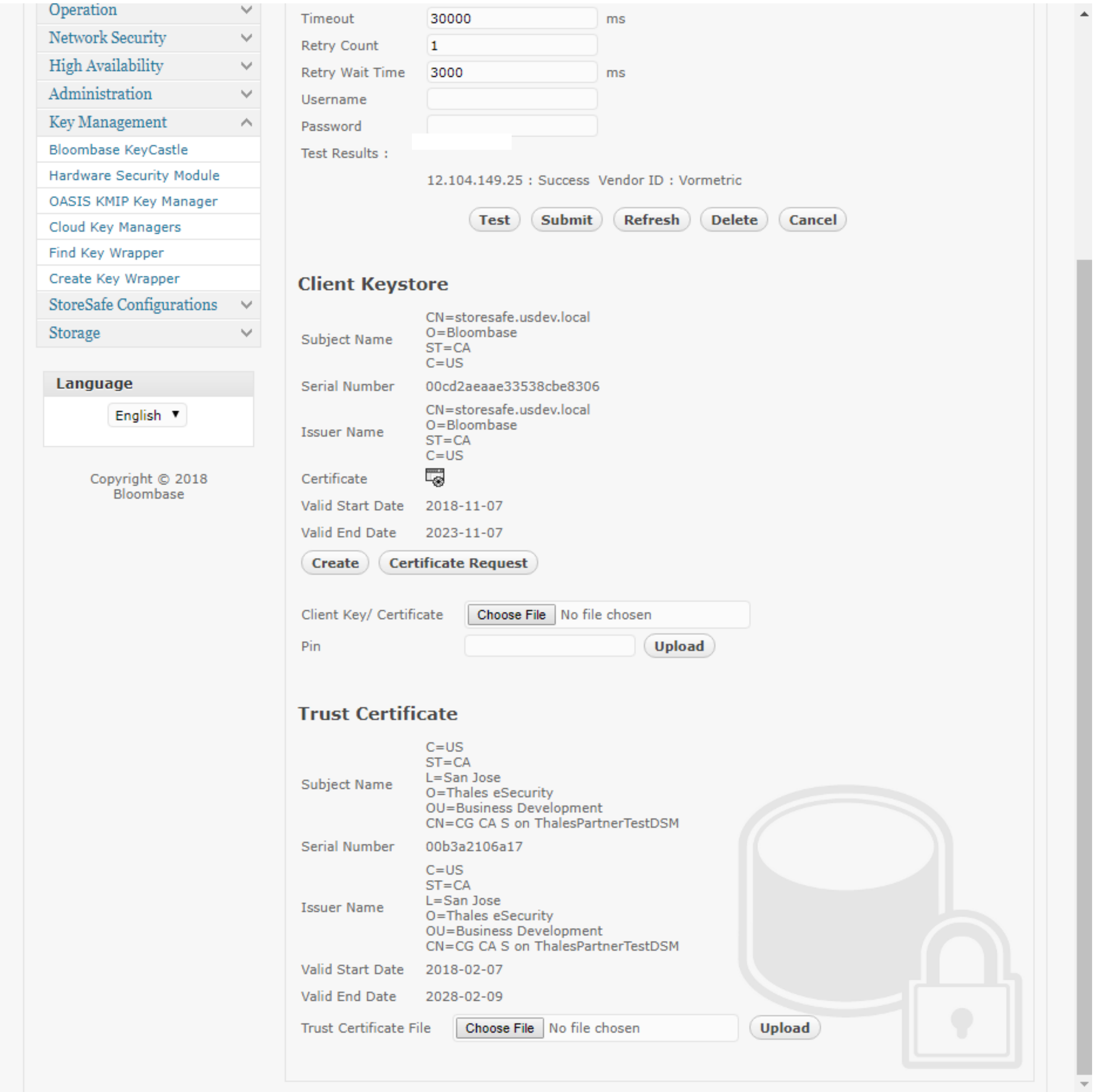
Client Keystore

Key Bit Length	2048
Signature Hash	SHA256
Country	US
State	CA
Locality	
Organization	Bloombase
Organizational Unit	
Common Name	storesafe.usdev.local

Trust Certificate

Subject Name	
Serial Number	
Issuer Name	
Valid Start Date	
Valid End Date	
Trust Certificate File	No file chosen

X.509 key pair `CN=storesafe.usdev.local` is generated and signed by the local root CA in the Thales Vormetric Data Security Manager (DSM) of distinguished name `C=US, ST=CA, L=San Jose, O=Thales eSecurity, OU=Business Development, CN=CG CA S on ThalesPartnerTestDSM`, and assigned as the client authentication key pair for Bloombase StoreSafe.



Timeout 30000 ms
Retry Count 1
Retry Wait Time 3000 ms
Username
Password
Test Results :

12.104.149.25 : Success Vendor ID : Vormetric

Client Keystore

Subject Name CN=storesafe.usdev.local
O=Bloombase
ST=CA
C=US

Serial Number 00cd2aeaae33538cbe8306

Issuer Name CN=storesafe.usdev.local
O=Bloombase
ST=CA
C=US

Certificate

Valid Start Date 2018-11-07

Valid End Date 2023-11-07

Client Key/ Certificate No file chosen

Pin

Trust Certificate

Subject Name C=US
ST=CA
L=San Jose
O=Thales eSecurity
OU=Business Development
CN=CG CA S on ThalesPartnerTestDSM

Serial Number 00b3a2106a17

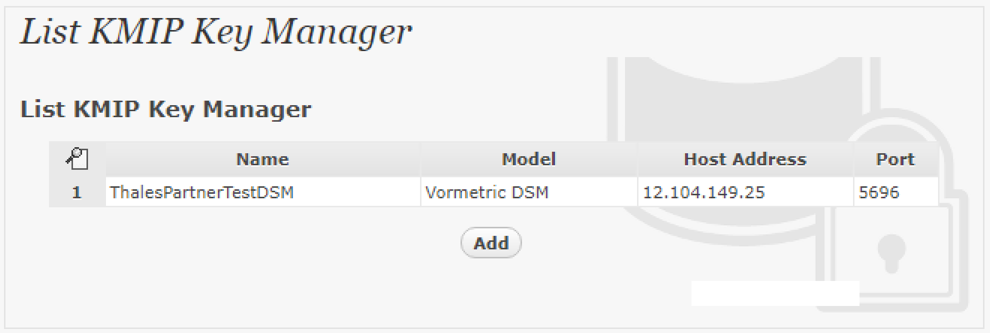
Issuer Name C=US
ST=CA
L=San Jose
O=Thales eSecurity
OU=Business Development
CN=CG CA S on ThalesPartnerTestDSM

Valid Start Date 2018-02-07

Valid End Date 2028-02-09

Trust Certificate File No file chosen

Click ‘Submit’ to commit the configuration. If the certificates are setup properly, “test results” of the KMIP Key Manager would return “Success”.



List KMIP Key Manager

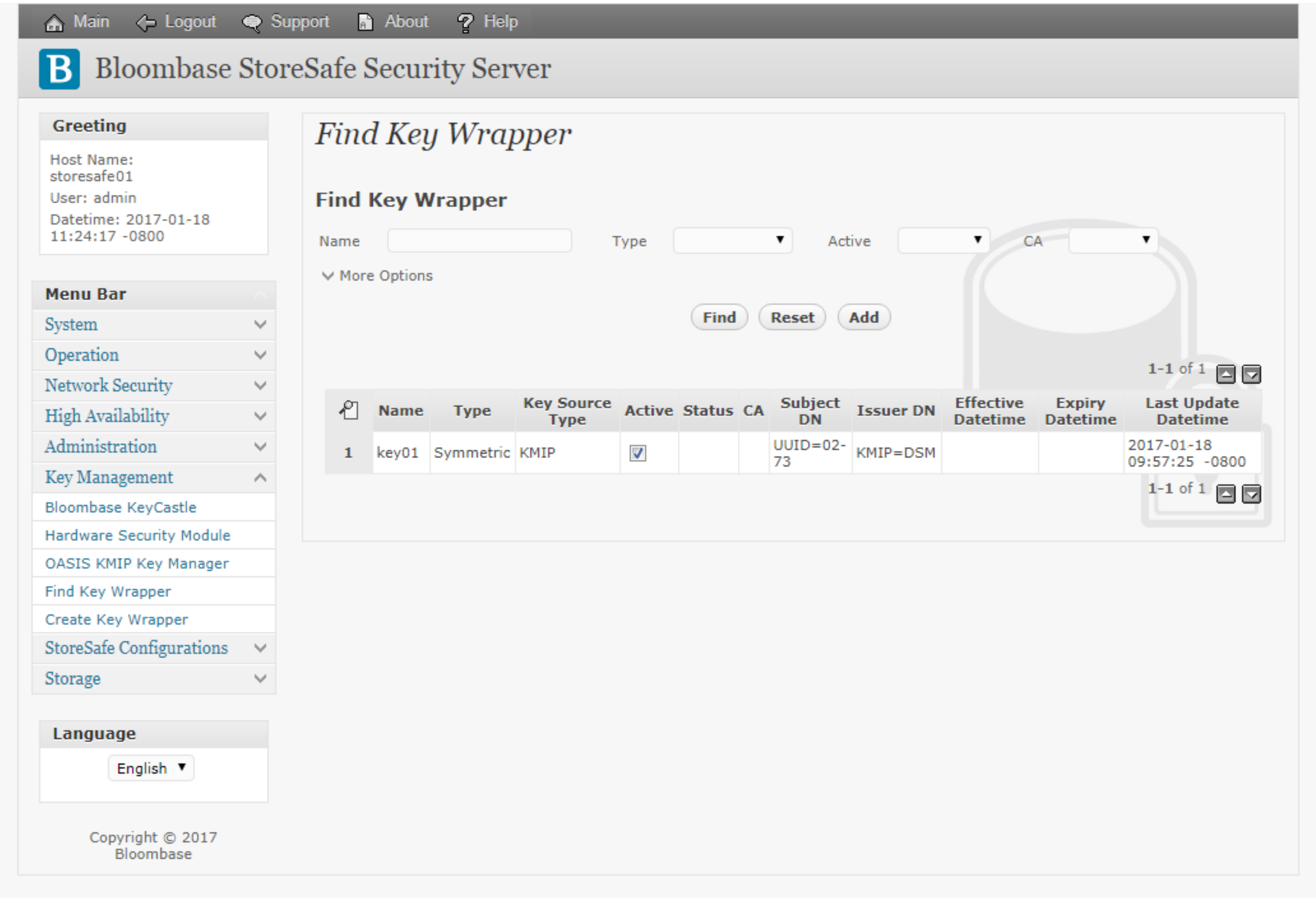
List KMIP Key Manager

	Name	Model	Host Address	Port
1	ThalesPartnerTestDSM	Vormetric DSM	12.104.149.25	5696

Encryption Key Provisioning

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

First configure the key source of the wrapping key as “OASIS KMIP Key Manager” with Thales Vormetric Data Security Manager (DSM) as the “Key Manager”.



Host Name: storesafe01
User: admin
Datetime: 2017-01-18 11:24:17 -0800

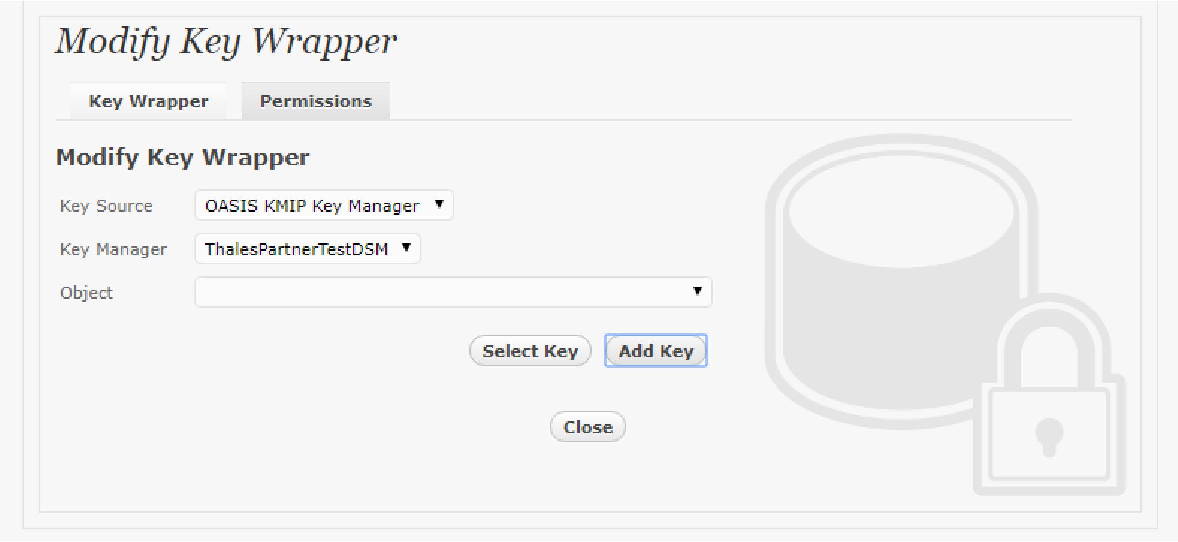
Find Key Wrapper

Find Key Wrapper

Name Type Active CA

	Name	Type	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1	key01	Symmetric	KMIP	☑			UUID=02-73	KMIP=DSM			2017-01-18 09:57:25 -0800

If the encryption key is present in the Thales Vormetric Data Security Manager (DSM), select from the dropdown menu of “Object” and click “submit”.



Modify Key Wrapper

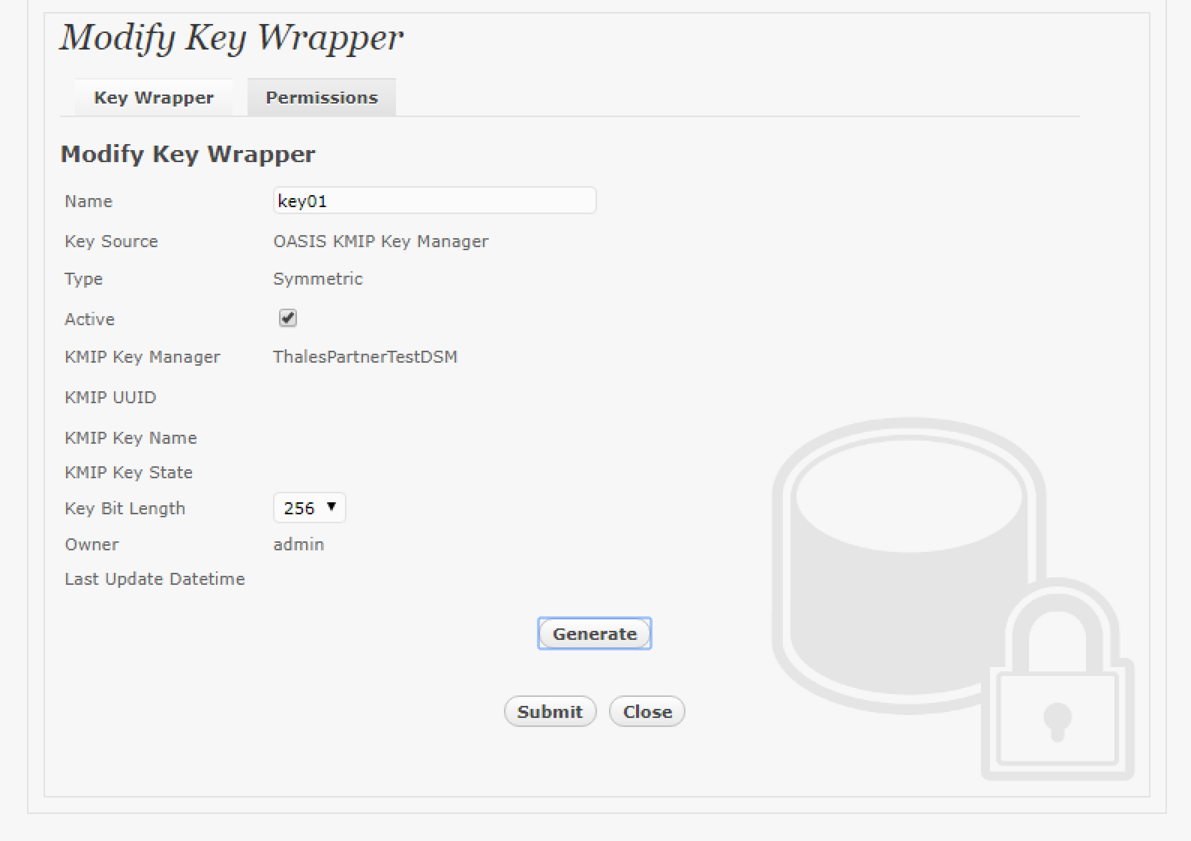
Modify Key Wrapper

Key Source: OASIS KMIP Key Manager

Key Manager: ThalesPartnerTestDSM

Object:

Otherwise, in order to generate the key in the attached Thales Vormetric Data Security Manager (DSM), leave the “Object” field as empty and click “Add Key” to input the name of the key and click ‘Generate’.

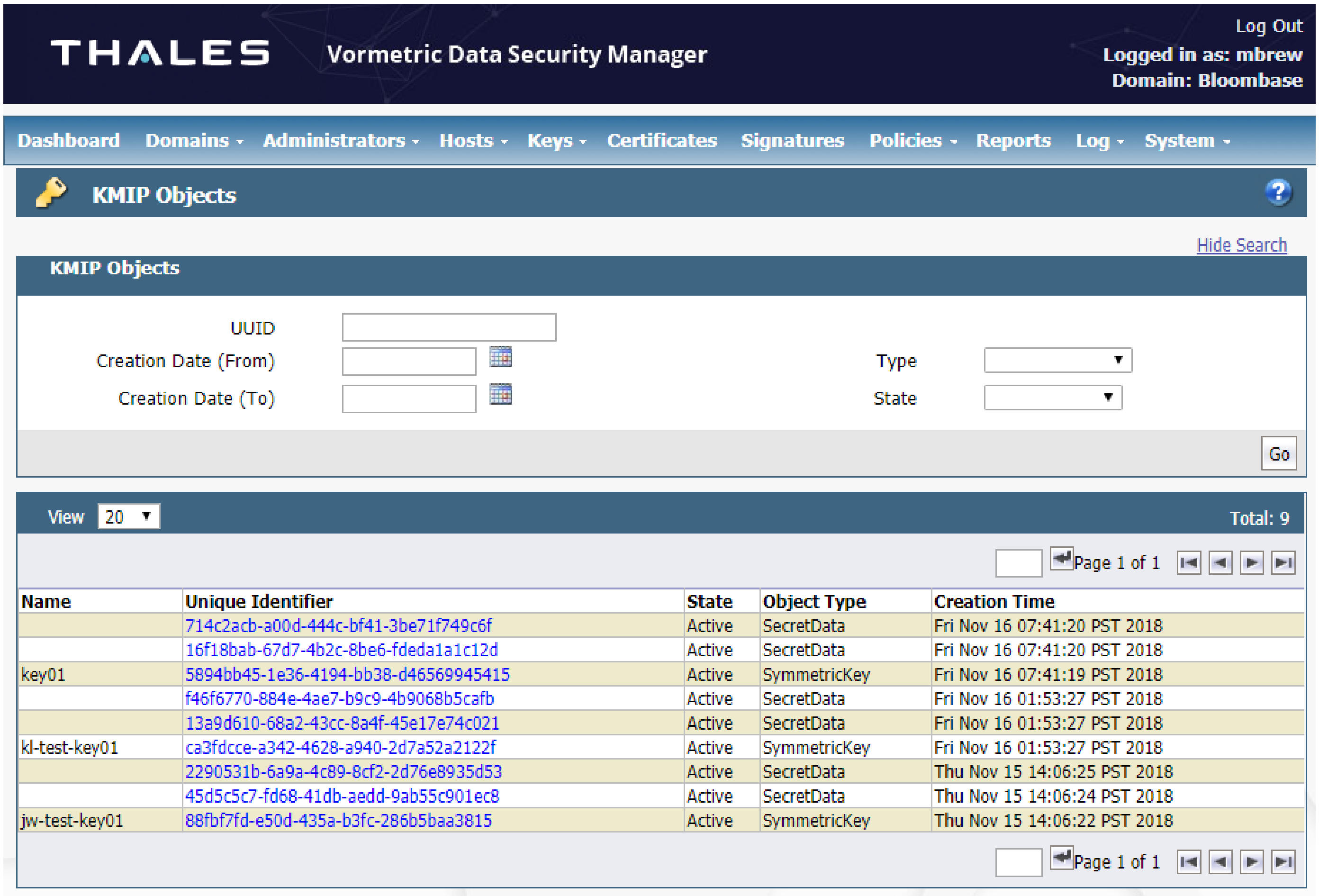


Modify Key Wrapper

Modify Key Wrapper

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

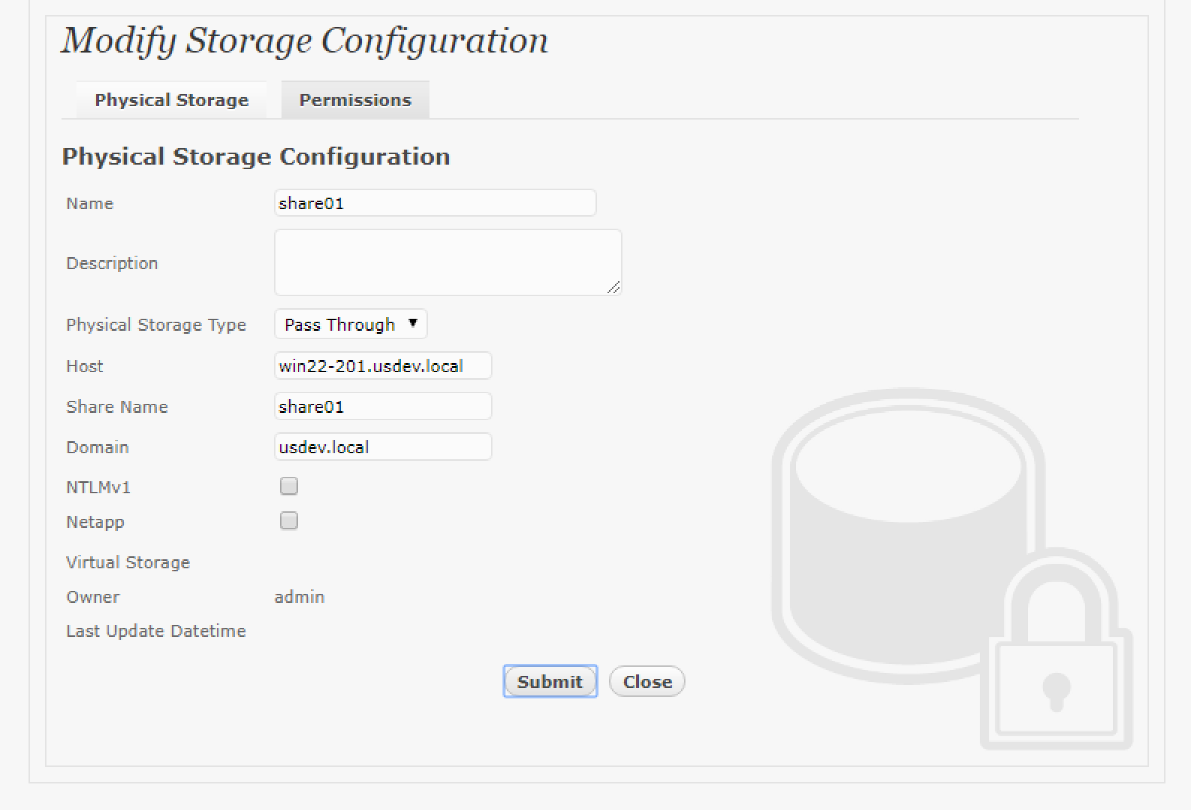
The key is then generated in the attached Thales Vormetric Data Security Manager (DSM).



Name	Unique Identifier	State	Object Type	Creation Time
	714c2acb-a00d-444c-bf41-3be71f749c6f	Active	SecretData	Fri Nov 16 07:41:20 PST 2018
	16f18bab-67d7-4b2c-8be6-fdeda1a1c12d	Active	SecretData	Fri Nov 16 07:41:20 PST 2018
key01	5894bb45-1e36-4194-bb38-d46569945415	Active	SymmetricKey	Fri Nov 16 07:41:19 PST 2018
	f46f6770-884e-4ae7-b9c9-4b9068b5cafb	Active	SecretData	Fri Nov 16 01:53:27 PST 2018
	13a9d610-68a2-43cc-8a4f-45e17e74c021	Active	SecretData	Fri Nov 16 01:53:27 PST 2018
kl-test-key01	ca3fdcce-a342-4628-a940-2d7a52a2122f	Active	SymmetricKey	Fri Nov 16 01:53:27 PST 2018
	2290531b-6a9a-4c89-8cf2-2d76e8935d53	Active	SecretData	Thu Nov 15 14:06:25 PST 2018
	45d5c5c7-fd68-41db-aedd-9ab55c901ec8	Active	SecretData	Thu Nov 15 14:06:24 PST 2018
jw-test-key01	88fbf7fd-e50d-435a-b3fc-286b5baa3815	Active	SymmetricKey	Thu Nov 15 14:06:22 PST 2018

Backend Physical Storage Configuration

Windows SMB physical storage namely `share01` is configured to be secured by Bloombase StoreSafe using encryption.

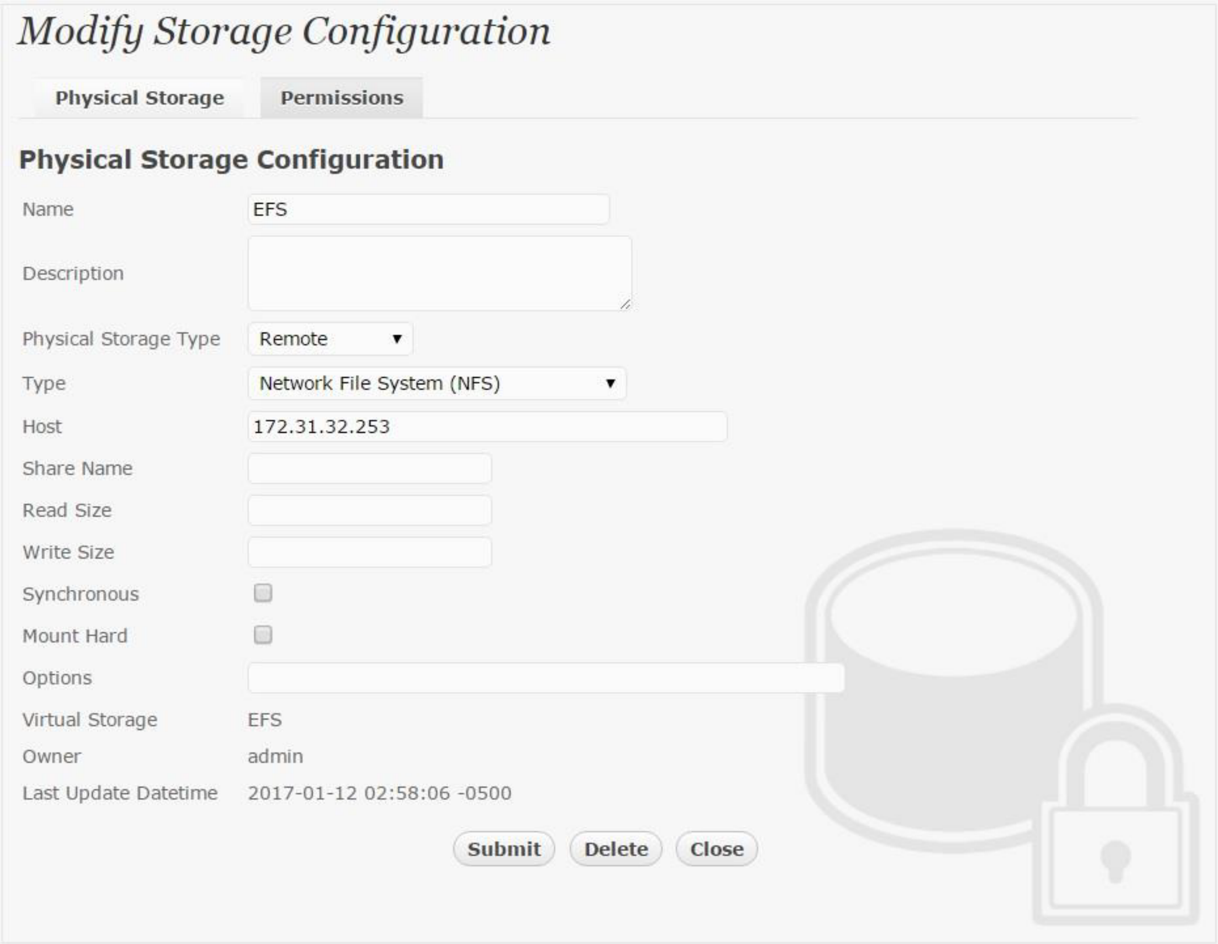


Modify Storage Configuration

Physical Storage Configuration

Name	share01
Description	
Physical Storage Type	Pass Through ▼
Host	win22-201.usdev.local
Share Name	share01
Domain	usdev.local
NTLMv1	□
Netapp	□
Virtual Storage	
Owner	admin
Last Update Datetime	

AWS EFS physical storage namely `EFS` is configured to be secured by Bloombase StoreSafe using encryption.

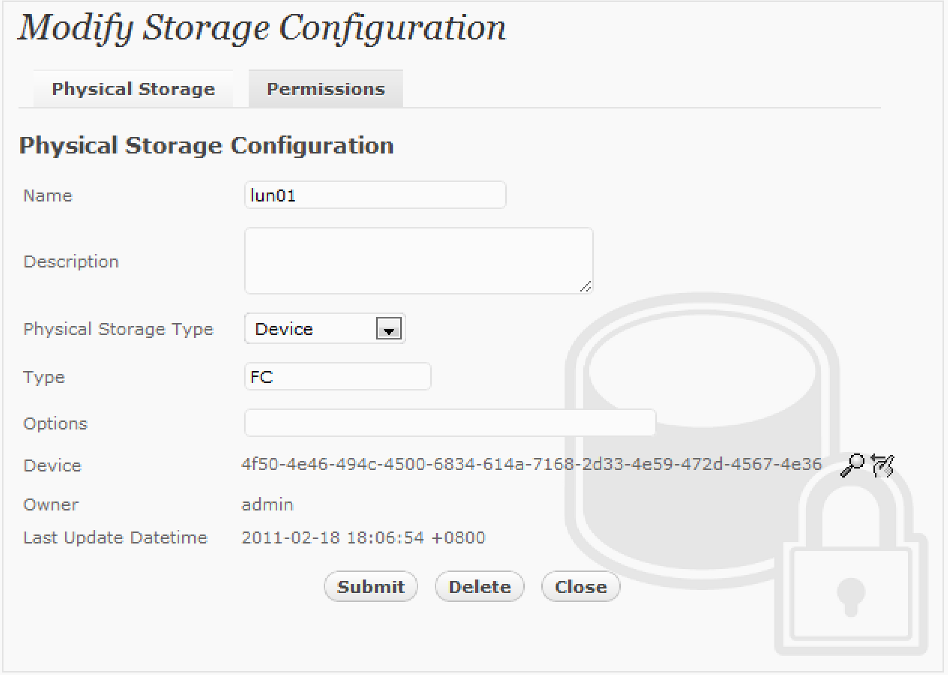


Modify Storage Configuration

Physical Storage Configuration

Name	EFS
Description	
Physical Storage Type	Remote ▾
Type	Network File System (NFS) ▾
Host	172.31.32.253
Share Name	
Read Size	
Write Size	
Synchronous	□
Mount Hard	□
Options	
Virtual Storage	EFS
Owner	admin
Last Update Datetime	2017-01-12 02:58:06 -0500

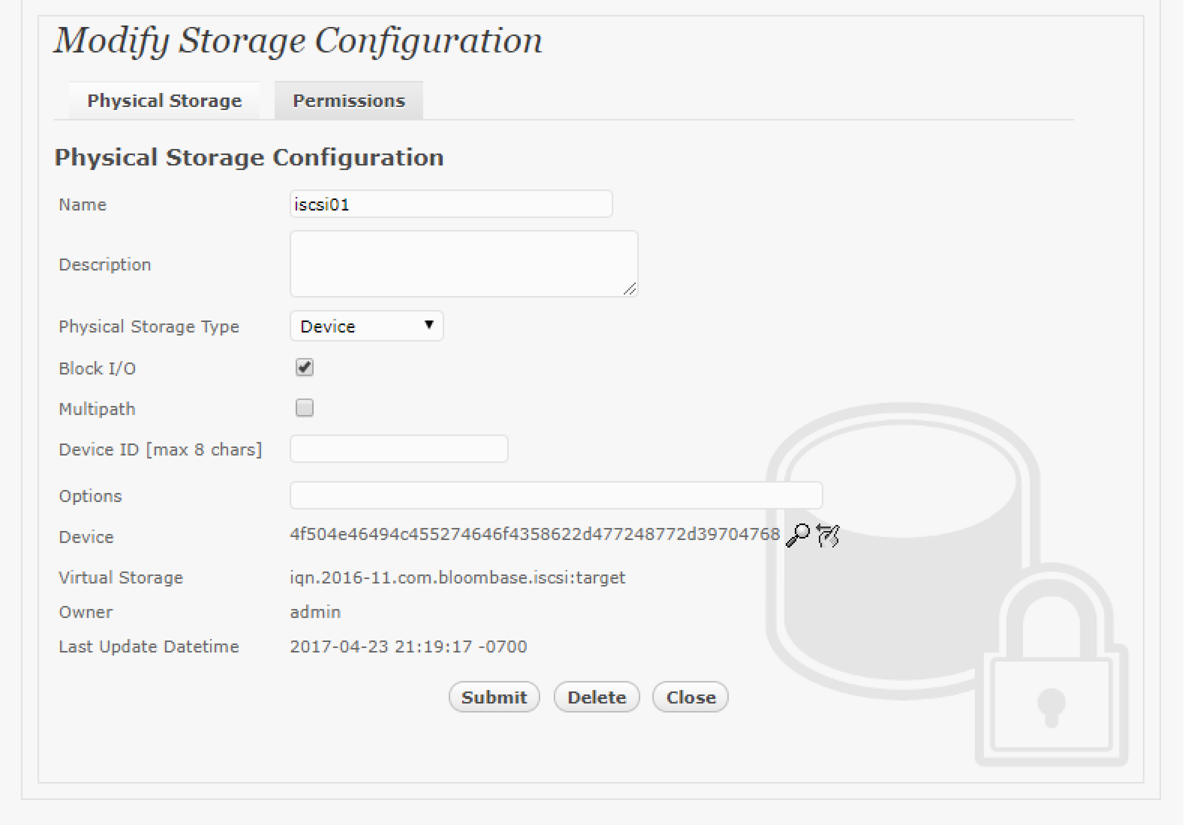
FCP physical storage namely `lun01` is configured to be secured by Bloombase StoreSafe using encryption.



Physical Storage Configuration

Name	lun01
Description	
Physical Storage Type	Device
Type	FC
Options	
Device	4f50-4e46-494c-4500-6834-614a-7168-2d33-4e59-472d-4567-4e36
Owner	admin
Last Update Datetime	2011-02-18 18:06:54 +0800

iSCSI physical storage namely `iscsi01` is configured to be secured by Bloombase StoreSafe using encryption.

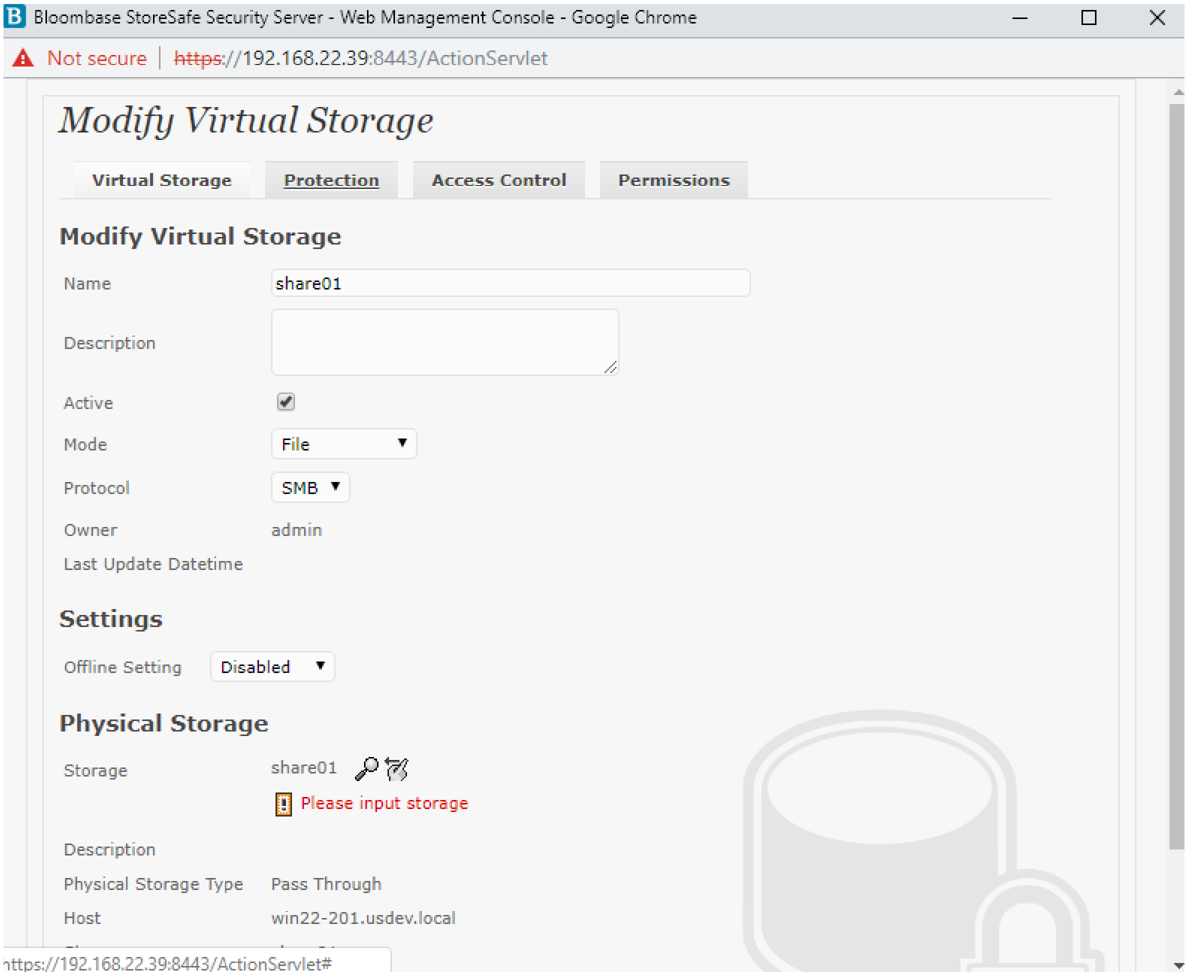


Physical Storage Configuration

Name	iscsi01
Description	
Physical Storage Type	Device
Block I/O	☑
Multipath	☐
Device ID [max 8 chars]	
Options	
Device	4f504e46494c455274646f4358622d477248772d39704768
Virtual Storage	iqn.2016-11.com.bloombase.iscsi:target
Owner	admin
Last Update Datetime	2017-04-23 21:19:17 -0700

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. Similar configurations are created for iSCSI, EFS, and FCP.



Bloombase StoreSafe Security Server - Web Management Console - Google Chrome
Not secure
~~https~~://192.168.22.39:8443/ActionServlet
Virtual Storage
Protection
Access Control
Permissions
https://192.168.22.39:8443/ActionServlet#

Modify Virtual Storage

Modify Virtual Storage

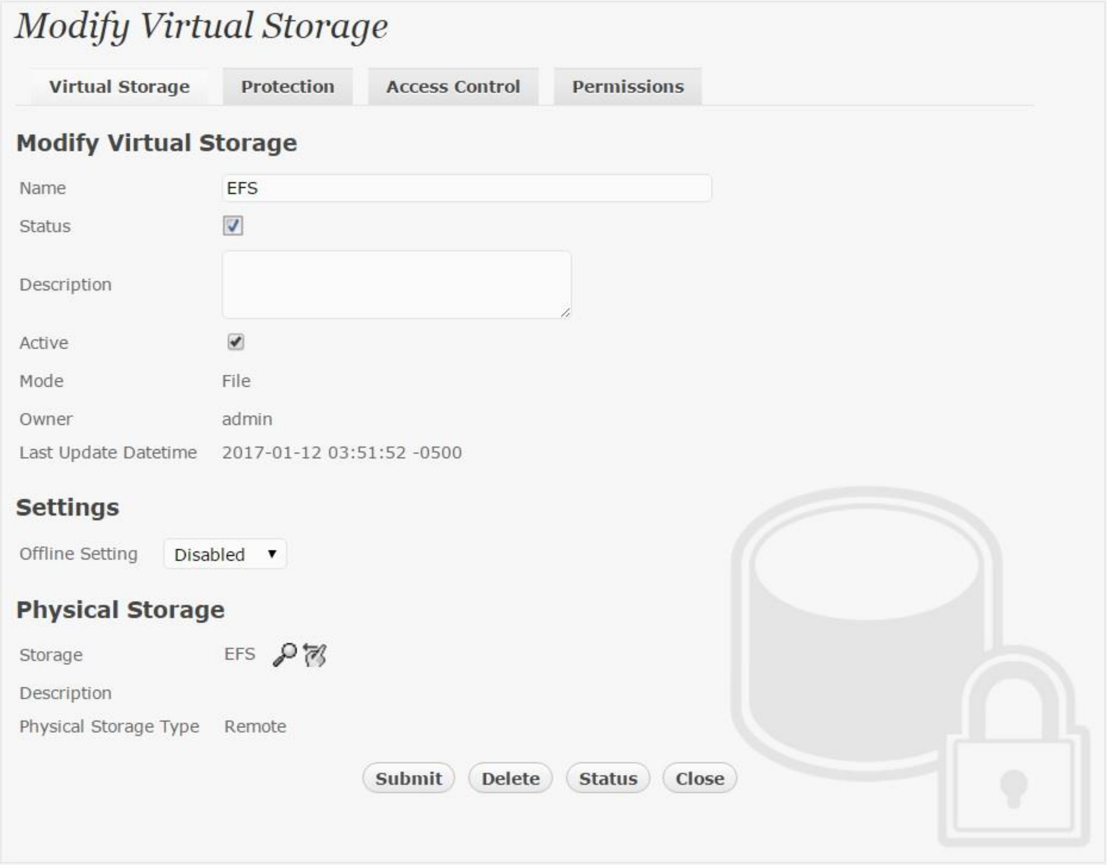
Name	share01
Description	
Active	☑
Mode	File
Protocol	SMB
Owner	admin
Last Update Datetime	

Settings

Offline Setting	Disabled

Physical Storage

Storage	share01 Please input storage
Description	
Physical Storage Type	Pass Through
Host	win22-201.usdev.local



Modify Virtual Storage

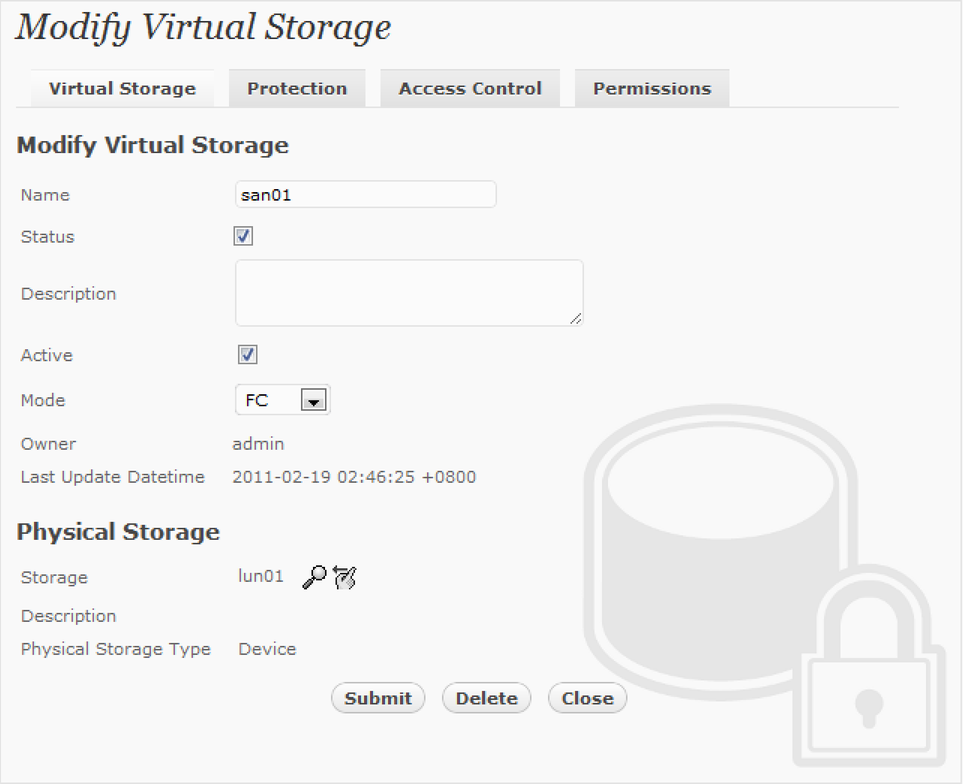
Name	EFS
Status	☑
Description	
Active	☑
Mode	File
Owner	admin
Last Update Datetime	2017-01-12 03:51:52 -0500

Settings

Offline Setting: Disabled

Physical Storage

Storage	EFS
Description	
Physical Storage Type	Remote

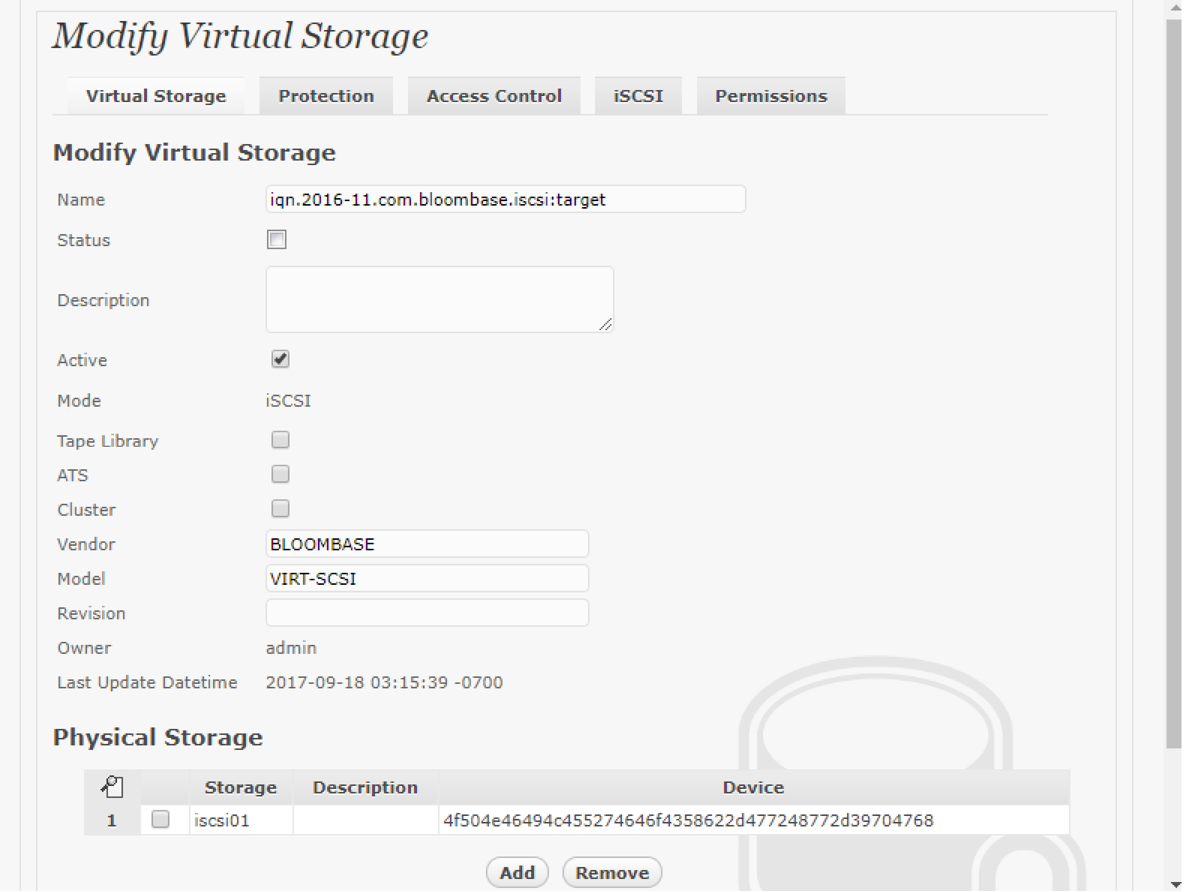


Modify Virtual Storage

Name	san01
Status	☑
Description	
Active	☑
Mode	FC
Owner	admin
Last Update Datetime	2011-02-19 02:46:25 +0800

Physical Storage

Storage	lun01
Description	
Physical Storage Type	Device



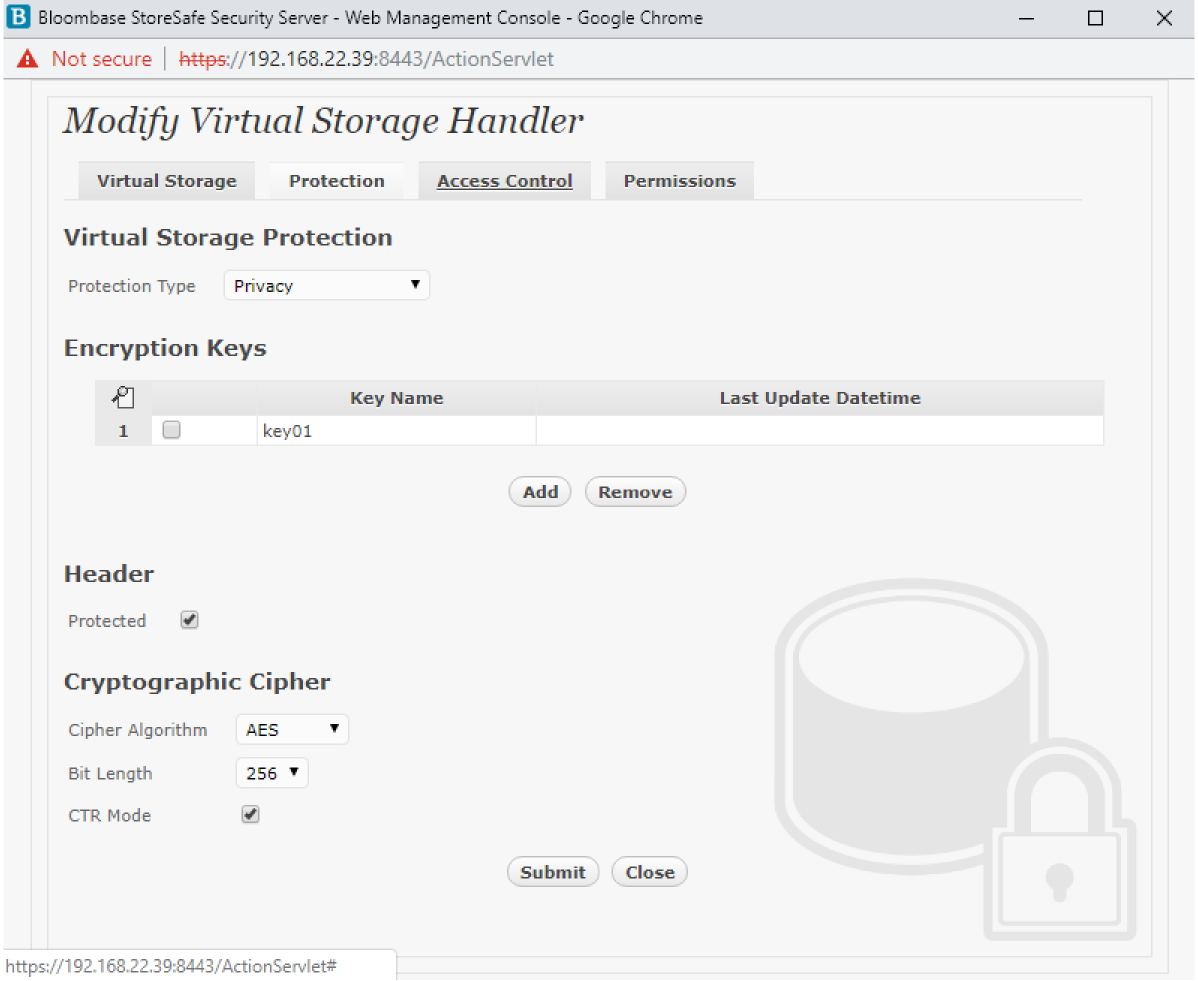
Modify Virtual Storage

Name	iqn.2016-11.com.bloombase.iscsi:target
Status	□
Description	
Active	☑
Mode	iSCSI
Tape Library	□
ATS	□
Cluster	□
Vendor	BLOOMBASE
Model	VIRT-SCSI
Revision	
Owner	admin
Last Update Datetime	2017-09-18 03:15:39 -0700

Physical Storage

		Storage	Description	Device
1	□	iscsi01		4f504e46494c455274646f4358622d477248772d39704768

Protection type is specified as `Privacy` and secure the backend Windows share or HPE P2000 G3 or Amazon S3 bucket using AES 256-bit encryption and encryption key `key01` managed at Thales Vormetric Data Security Manager (DSM).


Bloombase StoreSafe Security Server - Web Management Console - Google Chrome
Not secure | ~~https~~://192.168.22.39:8443/ActionServlet
Virtual Storage
Protection
Access Control
Permissions
Add
Remove
Submit
Close
https://192.168.22.39:8443/ActionServlet#

Modify Virtual Storage Handler

Virtual Storage Protection

Protection Type: Privacy

Encryption Keys

		Key Name	Last Update Datetime
1	□	key01	

Header

Protected ☑

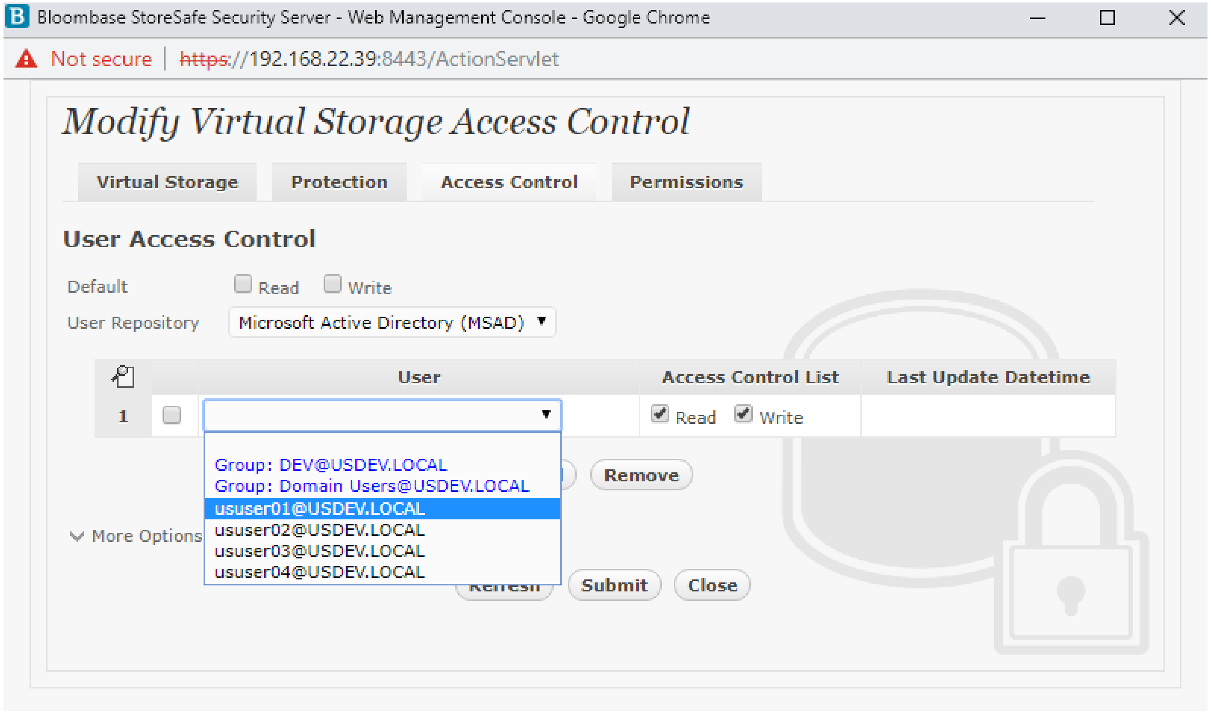
Cryptographic Cipher

Cipher Algorithm: AES

Bit Length: 256

CTR Mode ☑

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 `ususer01@USDEV.LOCAL` with Microsoft Active Directory integration for user-password authentication and single sign-on. Other protocols can utilize IP or other identifiers for access control.



Bloombase StoreSafe Security Server - Web Management Console - Google Chrome
Not secure
~~https~~://192.168.22.39:8443/ActionServlet
Virtual Storage
Protection
Access Control
Permissions
More Options
Remove
Submit
Close

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	□		☑ Read ☑ Write	

Group: DEV@USDEV.LOCAL
Group: Domain Users@USDEV.LOCAL
ususer01@USDEV.LOCAL
ususer02@USDEV.LOCAL
ususer03@USDEV.LOCAL
ususer04@USDEV.LOCAL

Conclusion

Key management system

- Thales Vormetric Data Security Manager (DSM)

passed all Bloombase interopLab's interoperability tests with Bloombase StoreSafe

Bloombase Product	Operating System	Key Management System
Bloombase StoreSafe	Microsoft Windows Server	Thales Vormetric Data Security Manager (DSM)
	Red Hat Enterprise Linux (RHEL)	Thales Vormetric Data Security Manager (DSM)
	SUSE Linux Enterprise Server (SLES)	Thales Vormetric Data Security Manager (DSM)
	Oracle Solaris	Thales Vormetric Data Security Manager (DSM)
	IBM AIX	Thales Vormetric Data Security Manager (DSM)
	HP-UX	Thales Vormetric Data Security Manager (DSM)

Disclaimer

The tests 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 differences in your configuration that will change the procedures necessary to accomplish the objectives outlined in this paper. If you find that any of these procedures do not work in your environment, please contact us immediately.

Acknowledgement

Bloombase InteropLab would like to thank Thales for supporting this interoperability testing.

Technical Reference

1. Bloombase StoreSafe Technical Specifications, http://www.bloombase.com/content/8936QA88

2. Bloombase StoreSafe Hardware Compatibility Matrix, http://www.bloombase.com/content/e8Gzz281

3. Blombase / Thales Data-at-Rest Encryption Solution, https://www.thalesesecurity.com/partners/bloombase

4. Thales Vormetric Data Security Manager (DSM), https://www.thalesesecurity.com/products/data-encryption/vormetric-data-security-manager

5. HPE P2000 MSA, https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c02020084

6. Microsoft Windows Server, https://www.microsoft.com/en-us/cloud-platform/windows-server

7. Amazon Elastic File System (EFS), https://aws.amazon.com/efs/

8. Amazon Simple Storage Service (S3), https://aws.amazon.com/s3/

9. Amazon Elastic Block Store (EBS), https://aws.amazon.com/ebs/

10. VMware ESXi, https://www.vmware.com/products/esxi-and-esx.htm

11. HPE OfficeConnect 1920 Switch Series, https://www.hpe.com/us/en/product-catalog/networking/networking-switches/pip.switches.7399514.html

12. OASIS Key Management Interoperability Protocol (KMIP), https://www.oasis-open.org/committees/kmip/