interopLab

Interoperability of Bloombase StoreSafe and Gemalto SafeNet ProtectServer for Data-at-Rest Encryption

May 2016

BLOOMBASE®

Executive Summary

Gemalto SafeNet ProtectServer Hardware Security Module (HSM) 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 Gemalto SafeNet ProtectServer HSM with Bloombase StoreSafe software appliance on VMware ESXi. 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 Gemalto SafeNet ProtectServer powered Bloombase StoreSafe with NetApp FAS unified storage system as backend storage.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, people and events depicted herein are fictitious and no association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Bloombase.

Bloombase may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Bloombase, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

This document is the property of Bloombase. No exploitation or transfer of any information contained herein is permitted in the absence of an agreement with Bloombase, and neither the document nor any such information may be released without the written consent of Bloombase.

Document No.: BLBS-TN-Bloombase-StoreSafe-Gemalto-SafeNet-ProtectServer-Interoperability-USLET-EN-R0.92

Table of Contents

Purpose and Scope

This document describes the steps necessary to integrate Gemalto SafeNet ProtectServer Hardware Security Module (HSM) with Bloombase StoreSafe to secure sensitive enterprise business data-at-rest managed in storage systems. Specifically, we cover the following topics:

- Install and configure Bloombase StoreSafe
- Integrate Bloombase StoreSafe with Gemalto SafeNet ProtectServer
- Interoperability testing on client host systems including Linux, Windows, IBM AIX, HP-UX and Oracle Sun Solaris

Assumptions

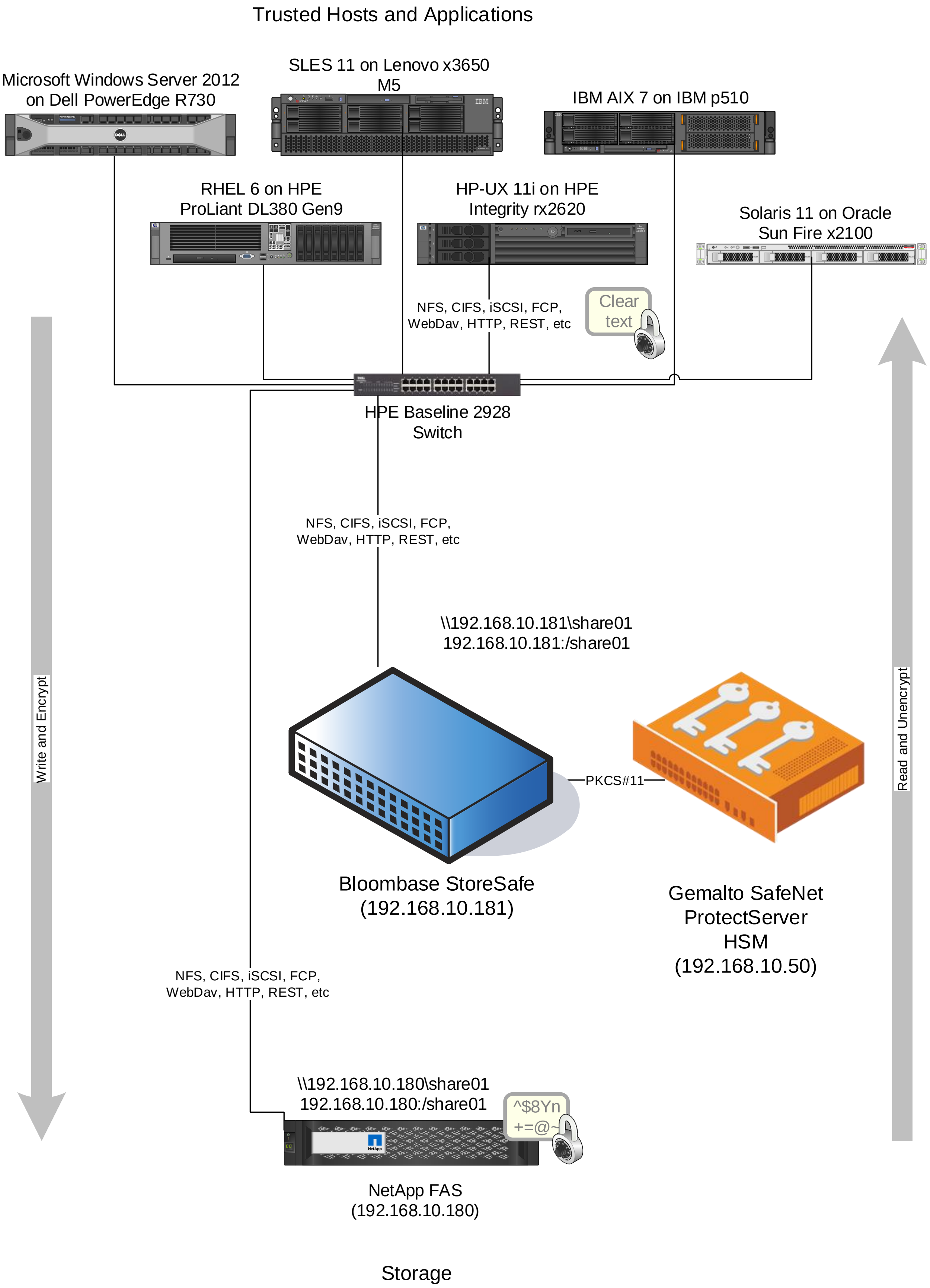
This document describes interoperability testing of Gemalto SafeNet ProtectServer Hardware Security Module (HSM) with Bloombase StoreSafe. Therefore, it is assumed that the reader is familiar with operation of Gemalto SafeNet ProtectServer HSM, storage systems and major operating systems including Linux, 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 Gemalto SafeNet ProtectServer HSM is a third party hardware 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 Gemalto SafeNet ProtectServer HSM 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 http://www.bloombase.com and Bloombase SupPortal http://supportal.bloombase.com.

Infrastructure

Setup

The validation testing environment is set up as in below diagram:


Trusted Hosts and Applications
Microsoft Windows Server 2012 on Dell PowerEdge R730
SLES 11 on Lenovo 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
NFS, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
Clear text
HPE Baseline 2928 Switch
Write and Encrypt
Read and Unencrypt
NFS, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
\\192.168.10.181\share01
192.168.10.181:/share01
PKCS#11
Bloombase StoreSafe (192.168.10.181)
Gemalto SafeNet ProtectServer HSM (192.168.10.50)
NFS, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
\\192.168.10.180\share01
192.168.10.180:/share01
^$8Yn +=@~
NetApp FAS (192.168.10.180)
Storage

Hardware Security Module

Hardware Security Module	Gemalto SafeNet ProtectServer External

Bloombase StoreSafe

Bloombase StoreSafe	Bloombase StoreSafe Software Appliance v3.5 on Bloombase OS 7
Server	VMware Virtual Machine (VM) on VMware ESXi 5.5
Processor	4 x Virtual CPU (vCPU)
Memory	8 GB

Storage System

Storage System	NetApp FAS Storage

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 2012	Red Hat Enterprise Linux 6	SUSE Linux Enterprise 11	HP-UX 11i	IBM AIX 7	Oracle Solaris 11

Configuration Overview

Gemalto SafeNet ProtectServer

Gemalto SafeNet ProtectServer Hardware Security Modules (HSMs) are designed to protect cryptographic keys against compromise while providing encryption, signing and authentication services to secure Java and sensitive web applications. Gemalto SafeNet ProtectServer HSMs offer a unique level of flexibility for application developers to create their own firmware and execute it within the secure confines of the HSM. Known as functionality modules, the toolkits provide a comprehensive facility to develop and deploy custom firmware. The key management and cryptographic functionalities provided by Gemalto SafeNet ProtectServer HSM are used by Bloombase StoreSafe for encryption protection of data-at-rest for general-purpose use cases.

Gemalto SafeNet ProtectServer Configurations

Assume Gemalto SafeNet ProtectServer is setup and configured as a network attached appliance with IP address 192.168.10.50.

Configure PKCS#11

After installing and configuring Network HSM Access Provider Software, `ETnethsm`, and ProtectToolkit C provided by SafeNet on Bloombase StoreSafe appliance, Gemalto SafeNet ProtectServer needs further configurations before Bloombase StoreSafe can communicate with it through PKCS#11. These configurations include creating a security officer (SO) for token initialization and creating an authorized user to use the token. Bloombase StoreSafe can then communicate with Gemalto SafeNet ProtectServer using the user account.

We setup an SO for token initialization and an administrator for HSM management, by running the following command.

```
ctconf
```

To disable unauthenticated usage of the HSM, run the following command.

```
ctconf -fc
```

To create one new user slot on the HSM, use the `ctconf` utility with the `–c` switch as follows.

```
ctconf –c1
```

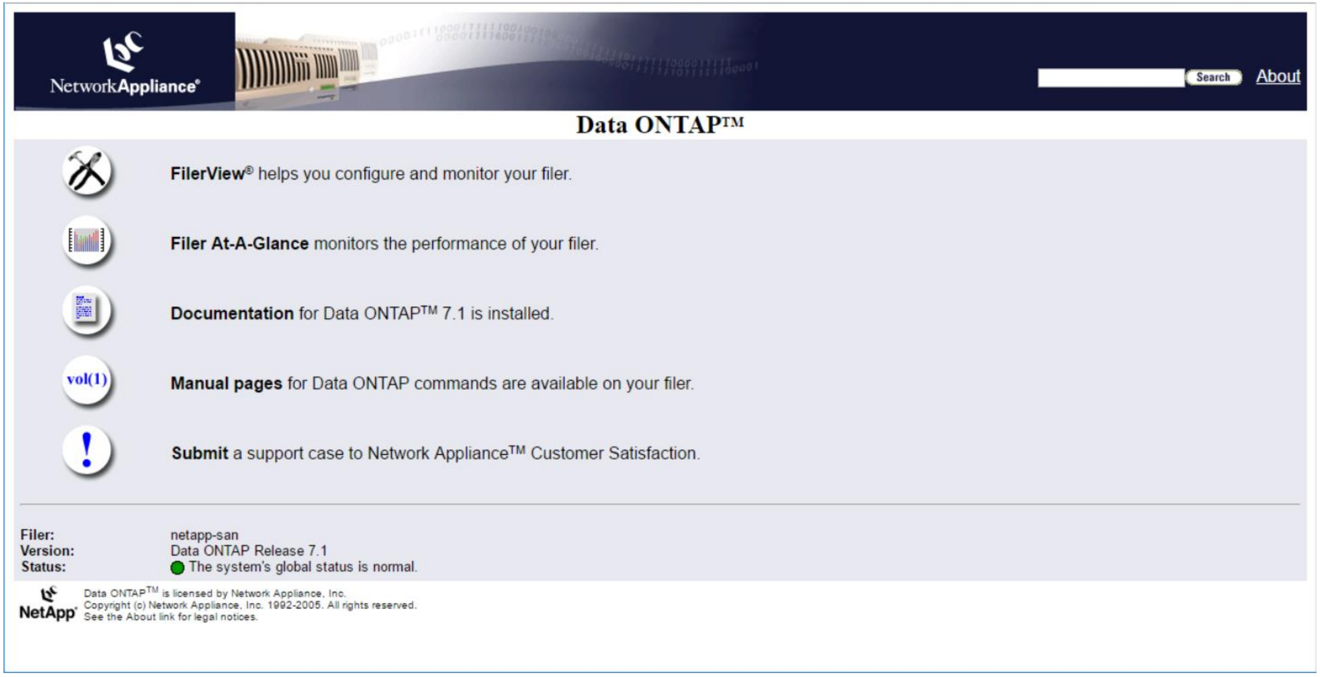
To initialize slot 0 and give it a unique token label “protectserver”, run the following command.

```
ctkmu t –s0 -lprotectserver
```

A user PIN is also setup when the above command is run. Use this user PIN to access the token from Bloombase StoreSafe.

NetApp FAS Storage

NetApp FAS virtual appliance is used in this interoperability test which is able to provide storage services over network storage protocols including NFS, CIFS, iSCSI, etc.



Data ONTAP™

FilerView® helps you configure and monitor your filer.

Filer At-A-Glance monitors the performance of your filer.

Documentation for Data ONTAP™ 7.1 is installed.

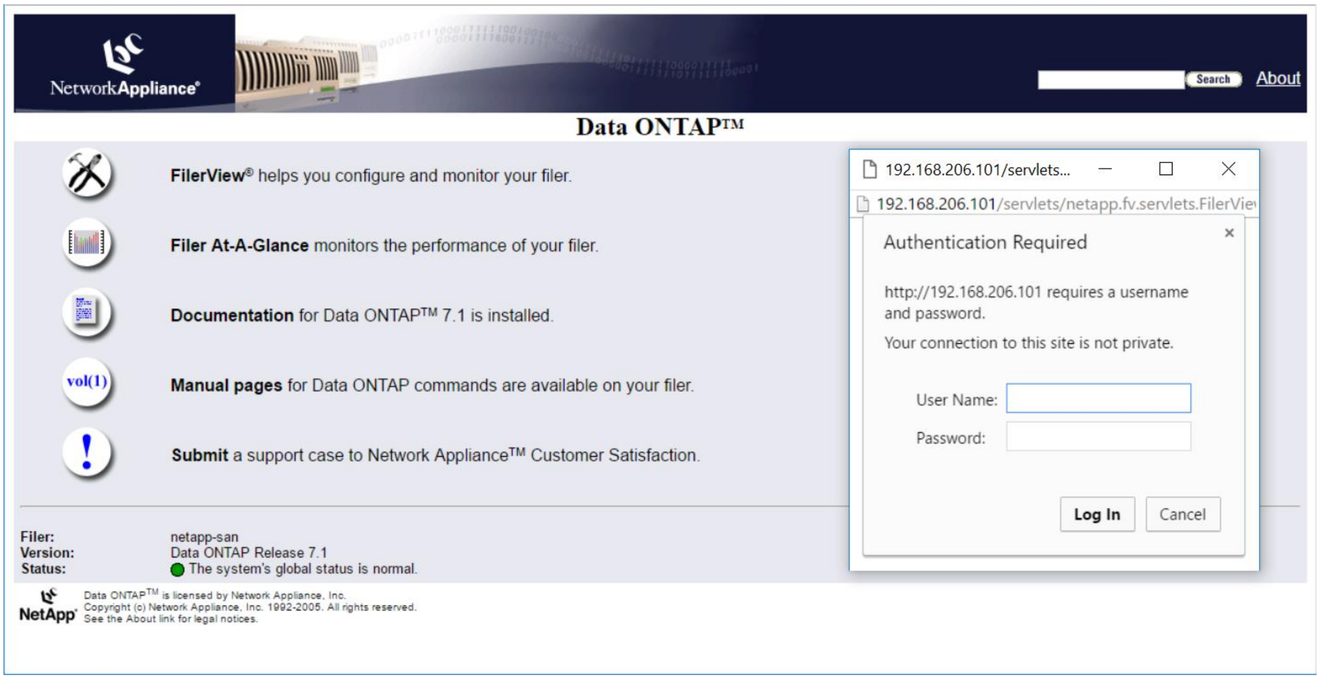
Manual pages for Data ONTAP commands are available on your filer.

Submit a support case to Network Appliance™ Customer Satisfaction.

Filer: netapp-san
Version: Data ONTAP Release 7.1
Status: ● The system's global status is normal.

NetApp® Data ONTAP™ is licensed by Network Appliance, Inc. Copyright (c) Network Appliance, Inc. 1992-2005. All rights reserved. See the About link for legal notices.

NetApp FAS is a unified storage system supporting multiple network storage protocols including NFS, CIFS, HTTP, FC, FCoE, iSCSI, etc.



Data ONTAP™

FilerView® helps you configure and monitor your filer.

Filer At-A-Glance monitors the performance of your filer.

Documentation for Data ONTAP™ 7.1 is installed.

Manual pages for Data ONTAP commands are available on your filer.

Submit a support case to Network Appliance™ Customer Satisfaction.

Filer: netapp-san
Version: Data ONTAP Release 7.1
Status: ● The system's global status is normal.

NetApp® Data ONTAP™ is licensed by Network Appliance, Inc. Copyright (c) Network Appliance, Inc. 1992-2005. All rights reserved. See the About link for legal notices.

192.168.206.101/servlets...

192.168.206.101/servlets/netapp.fv.servlets.FilerVie

Authentication Required

http://192.168.206.101 requires a username and password.

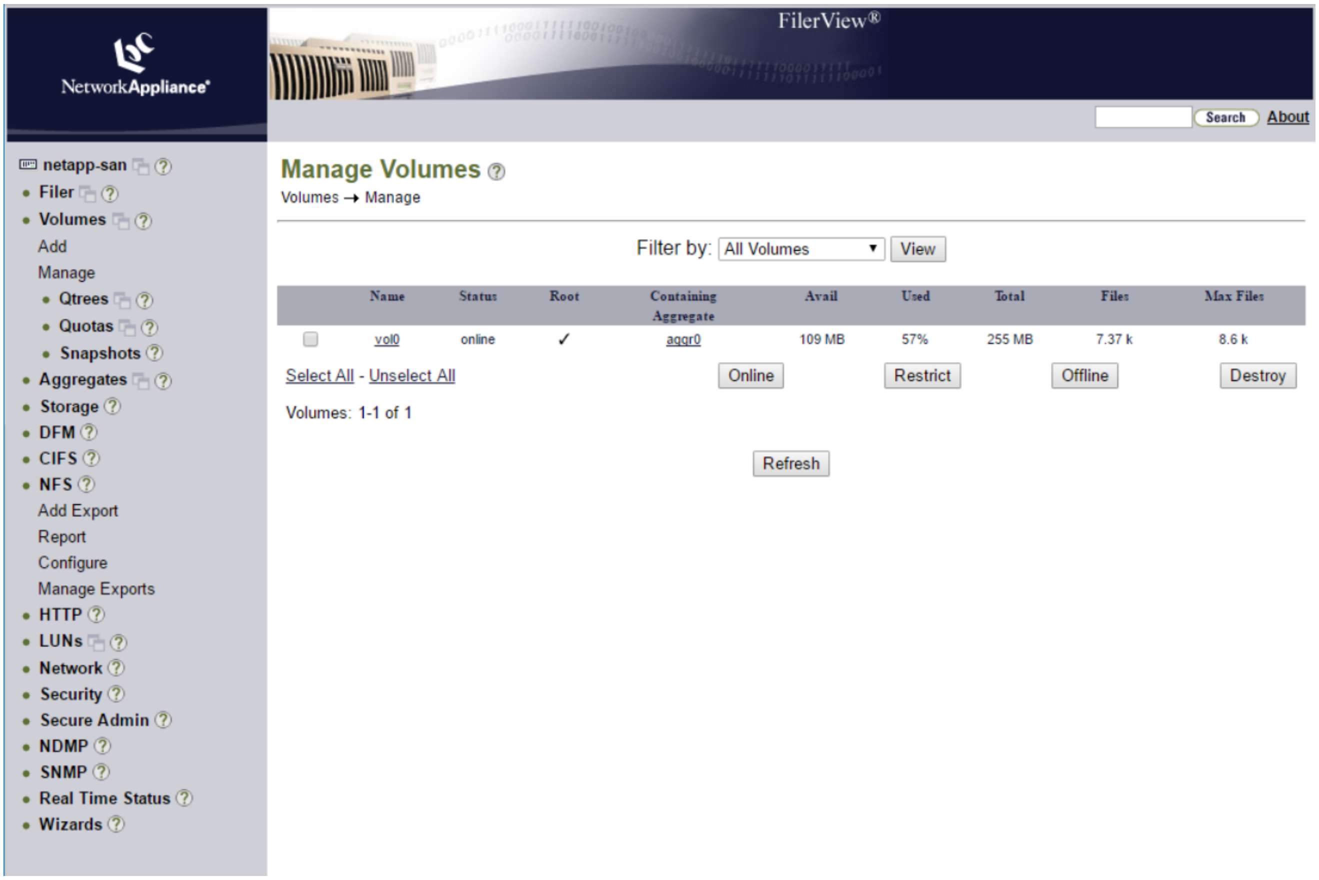
Your connection to this site is not private.

User Name:

Password:

Log In Cancel

CIFS and NFS storage resources are provisioned on NetApp FAS to be used in this testing.



Manage Volumes

Volumes → Manage

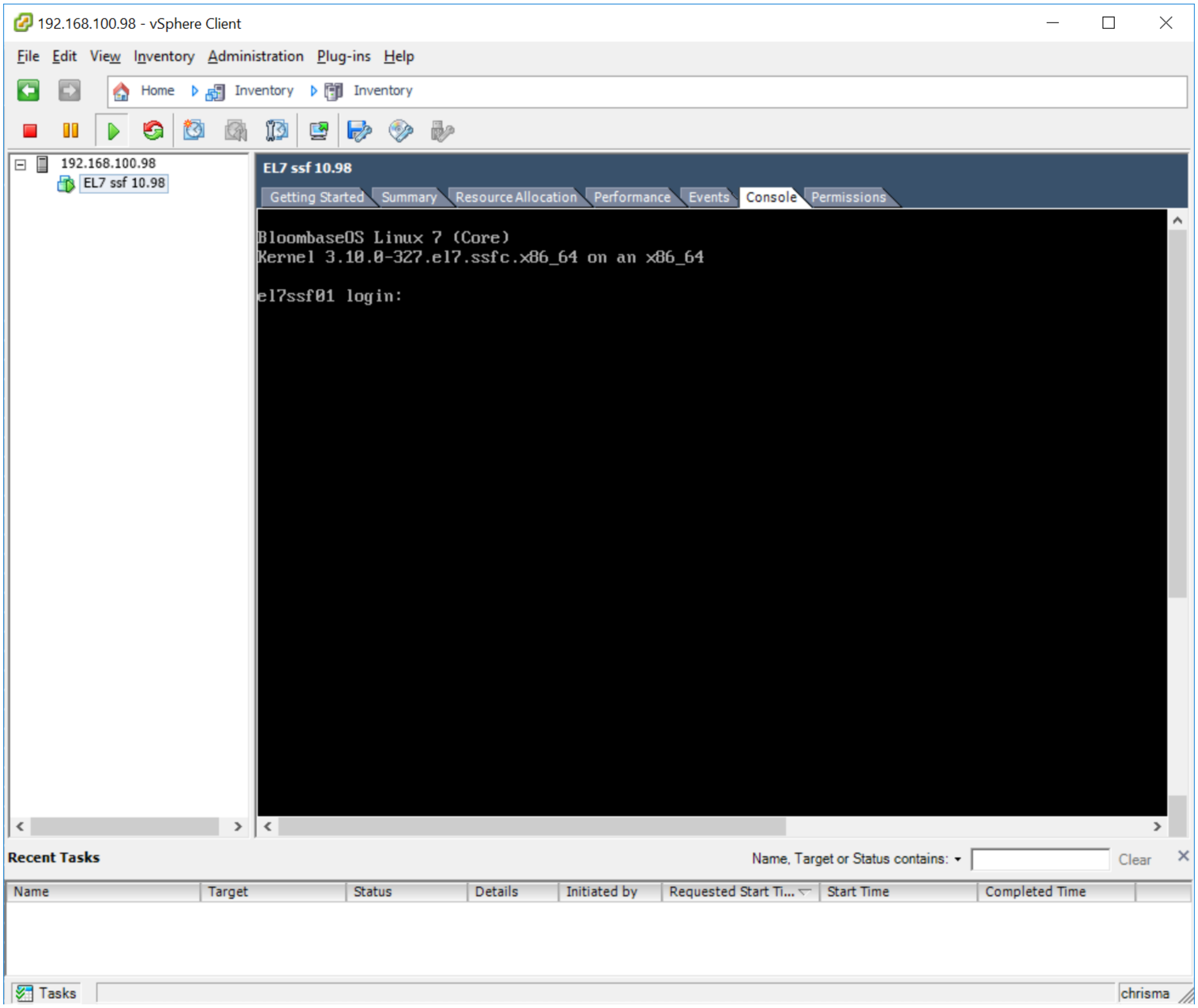
Filter by: All Volumes

	Name	Status	Root	Containing Aggregate	Avail	Used	Total	Files	Max Files
□	vol0	online	✓	aggr0	109 MB	57%	255 MB	7.37 k	8.6 k

Volumes: 1-1 of 1

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 Gemalto SafeNet ProtectServer.


192.168.100.98 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
192.168.100.98
EL7 ssf 10.98
EL7 ssf 10.98
Getting Started Summary Resource Allocation Performance Events Console Permissions
Recent Tasks
Name, Target or Status contains:
Clear
Name Target Status Details Initiated by Requested Start Ti... Start Time Completed Time
Tasks
chrisma

```
BloombaseOS Linux 7 (Core)
Kernel 3.10.0-327.el7.ssfc.x86_64 on an x86_64

el7ssf01 login:
```

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

Network Security, Trust and Authentication Configuration

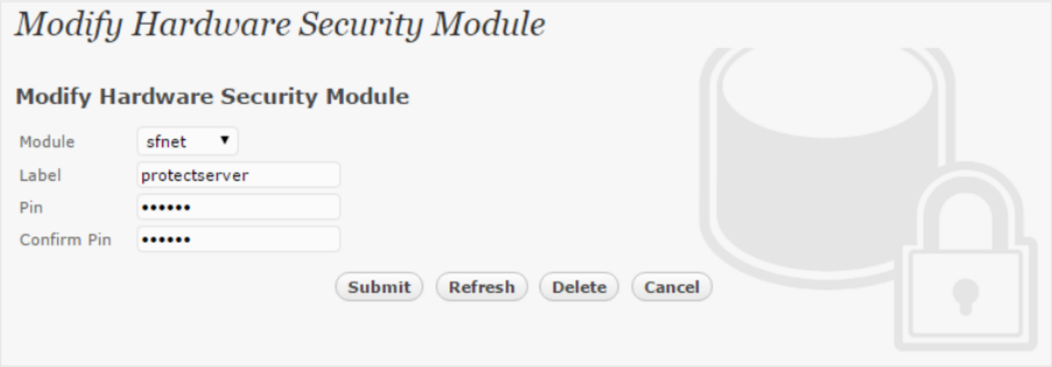
In this interoperability test effort, Bloombase StoreSafe serves as the user of Gemalto SafeNet ProtectServer HSM for encryption key access to deliver data at-rest encryption services. Authentication of Bloombase StoreSafe to the Gemalto SafeNet ProtectServer HSM is done through the specification of user pin.

Gemalto SafeNet ProtectServer HSM and Bloombase KeyCastle Integration

We first set the environment variable `ET_HSM_NETCLIENT_SERVERLIST` with the IP address and port of Gemalto SafeNet ProtectServer, e.g.,

```
export ET_HSM_NETCLIENT_SERVERLIST=192.168.10.50:12396
```

To configure Gemalto SafeNet ProtectServer HSM at Bloombase web management console, select Module as 'sfnet' which allows the embedded Bloombase KeyCastle module to utilize Gemalto SafeNet ProtectServer driver to access Gemalto SafeNet ProtectServer over standard PKCS#11 protocol.

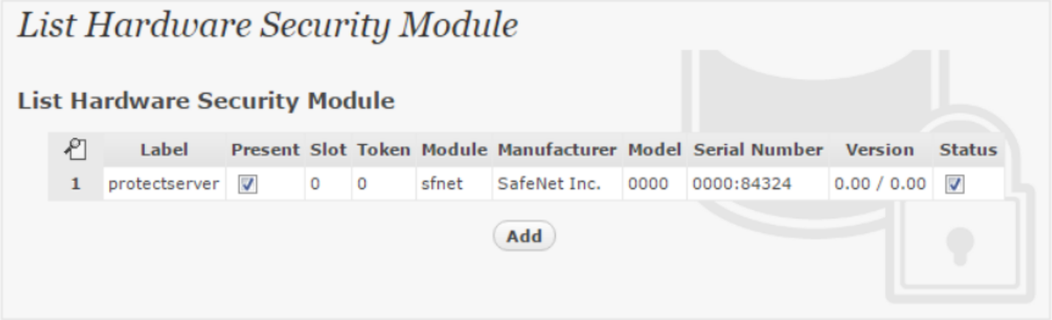


Modify Hardware Security Module

Modify Hardware Security Module

Module	sfnet
Label	protectserver
Pin	••••••
Confirm Pin	••••••

In this scenario, use the Gemalto SafeNet ProtectServer HSM with a token label 'protectserver' and user pin as Pin. When Gemalto SafeNet ProtectServer HSM resource is properly provisioned at Bloombase StoreSafe, the status would show up as 'Active'.



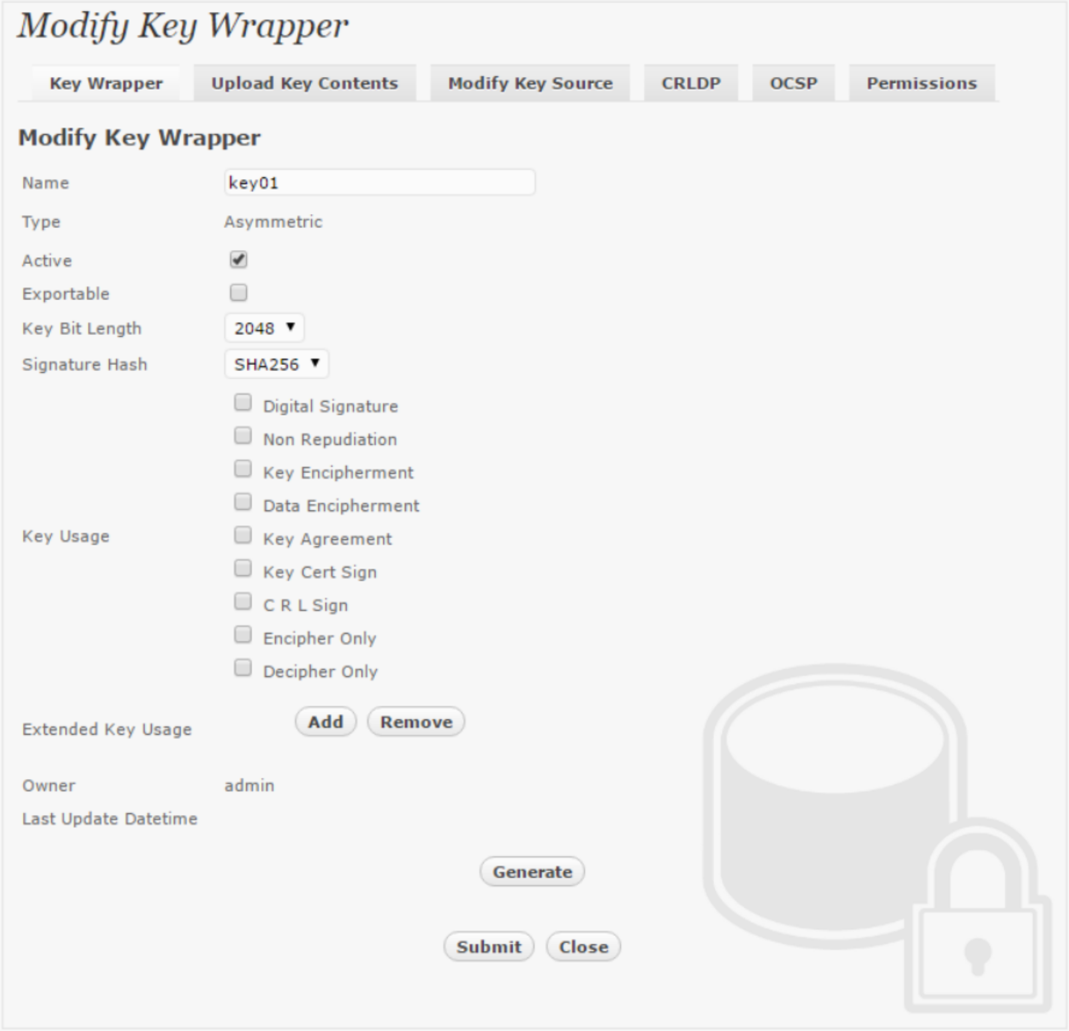
List Hardware Security Module

List Hardware Security Module

	Label	Present	Slot	Token	Module	Manufacturer	Model	Serial Number	Version	Status
1	protectserver	☑	0	0	sfnet	SafeNet Inc.	0000	0000:84324	0.00 / 0.00	☑

Encryption Key Provisioning

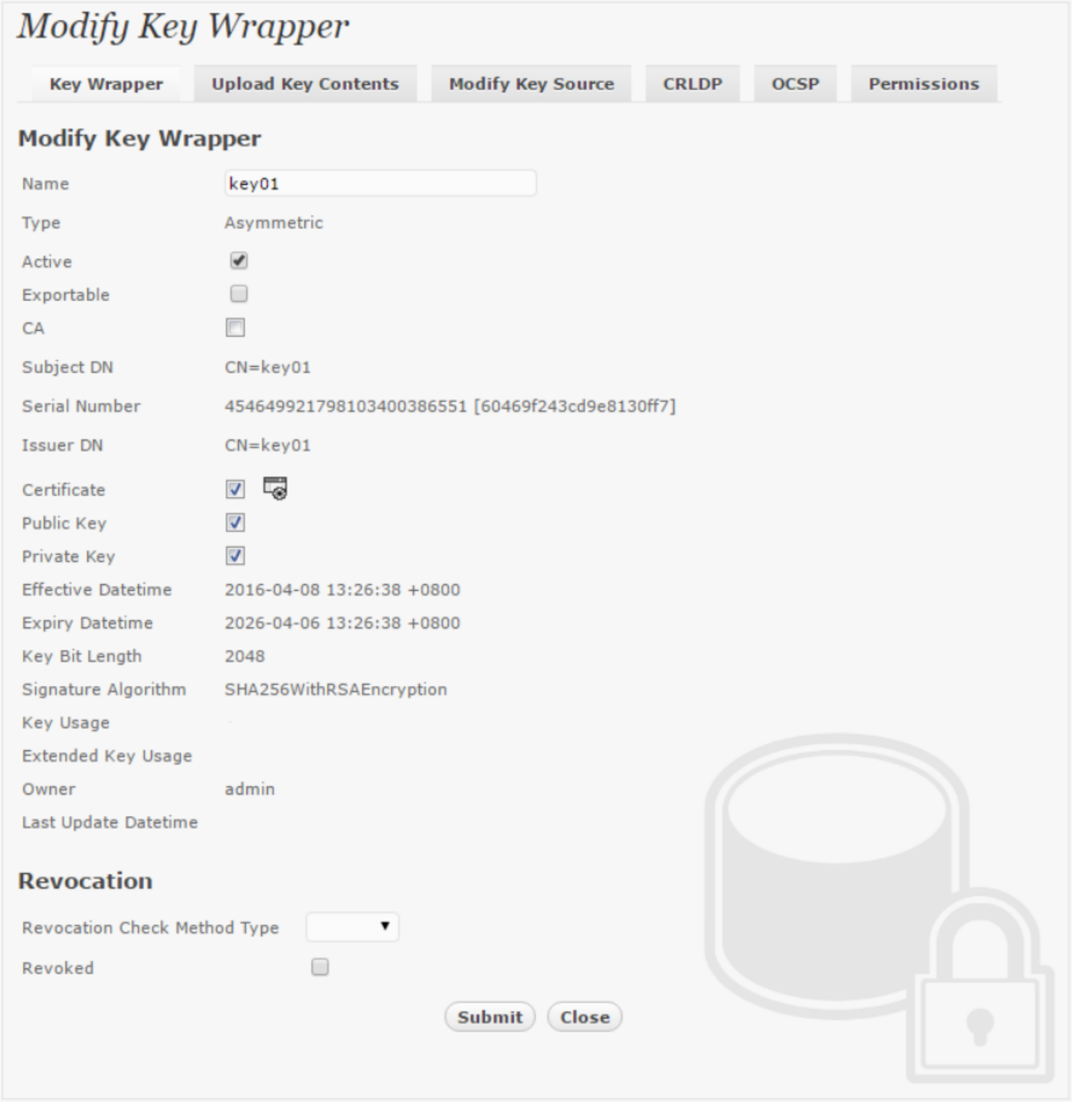
Generate encryption key with name ‘key01’ in bundled Bloombase KeyCastle key life-cycle management tool



Modify Key Wrapper

Name	key01
Type	Asymmetric
Active	☑
Exportable	☐
Key Bit Length	2048 ▼
Signature Hash	SHA256 ▼
Key Usage	☐ Digital Signature ☐ Non Repudiation ☐ Key Encipherment ☐ Data Encipherment ☐ Key Agreement ☐ Key Cert Sign ☐ C R L Sign ☐ Encipher Only ☐ Decipher Only
Extended Key Usage	
Owner	admin
Last Update Datetime	

To generate key in attached Gemalto SafeNet ProtectServer HSM, input details of the key and click ‘Generate’.



Modify Key Wrapper

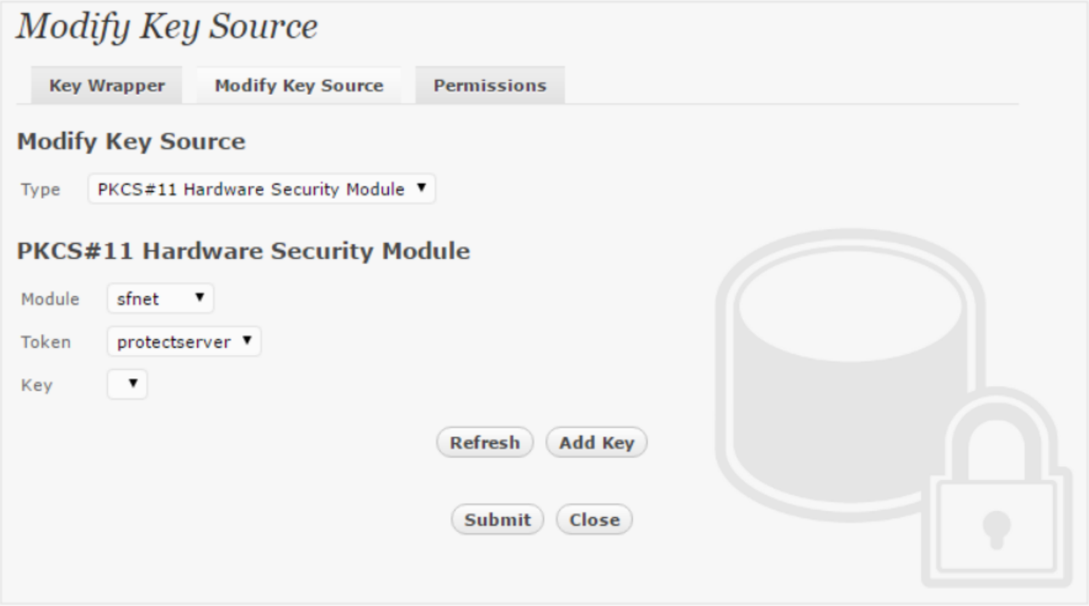
Modify Key Wrapper

Name	key01
Type	Asymmetric
Active	☑
Exportable	□
CA	□
Subject DN	CN=key01
Serial Number	454649921798103400386551 [60469f243cd9e8130ff7]
Issuer DN	CN=key01
Certificate	☑
Public Key	☑
Private Key	☑
Effective Datetime	2016-04-08 13:26:38 +0800
Expiry Datetime	2026-04-06 13:26:38 +0800
Key Bit Length	2048
Signature Algorithm	SHA256WithRSAEncryption
Key Usage	
Extended Key Usage	
Owner	admin
Last Update Datetime	

Revocation

Revocation Check Method Type	▾
Revoked	□

Then click ‘Modify Key Source’ and select Key Source Type as ‘PKCS#11 Hardware Security Module’, Module as ‘sfnet’ and the assigned HSM token label, in this case ‘protectserver’.



Modify Key Source

Type: PKCS#11 Hardware Security Module

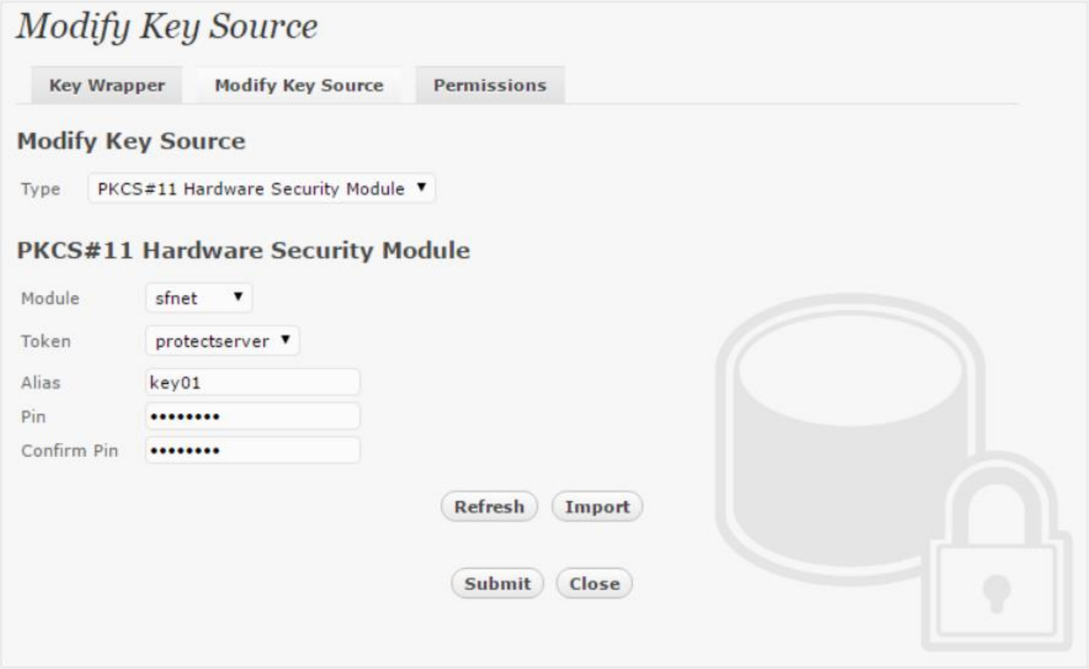
PKCS#11 Hardware Security Module

Module: sfnet

Token: protectserver

Key:

Select ‘Add Key’ to input a unique alias as the key name, and input the user pin of the token to import a new key from the HSM before you submit the key wrapper.



Modify Key Source

Type: PKCS#11 Hardware Security Module

PKCS#11 Hardware Security Module

Module: sfnet

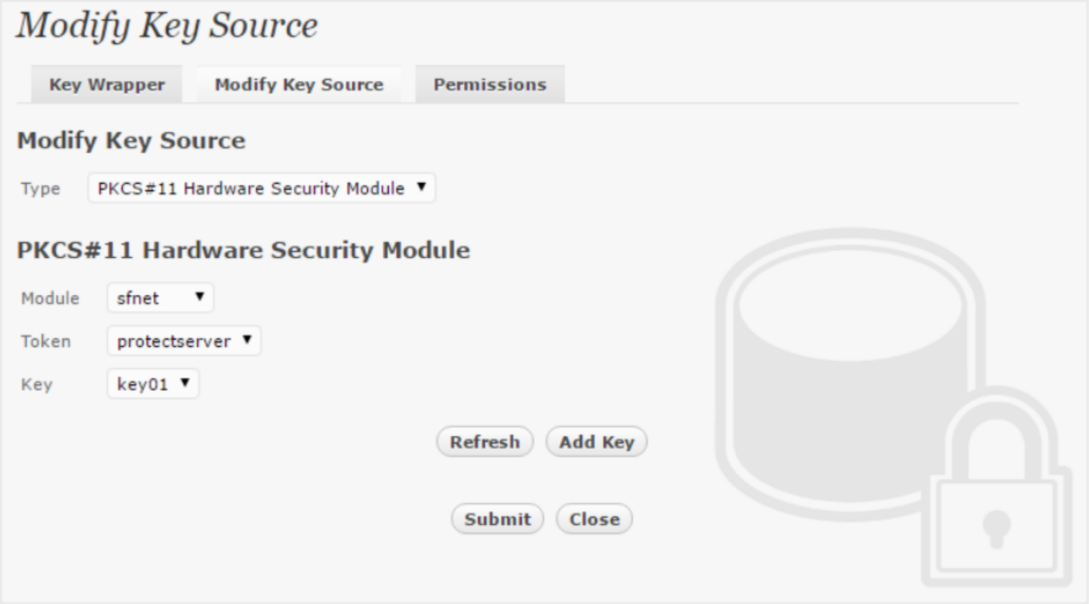
Token: protectserver

Alias: key01

Pin: ••••••••

Confirm Pin: ••••••••

Or if key already exists in the HSM, simply choose from the pull down box and click ‘Add Key’.



Modify Key Source

Type PKCS#11 Hardware Security Module

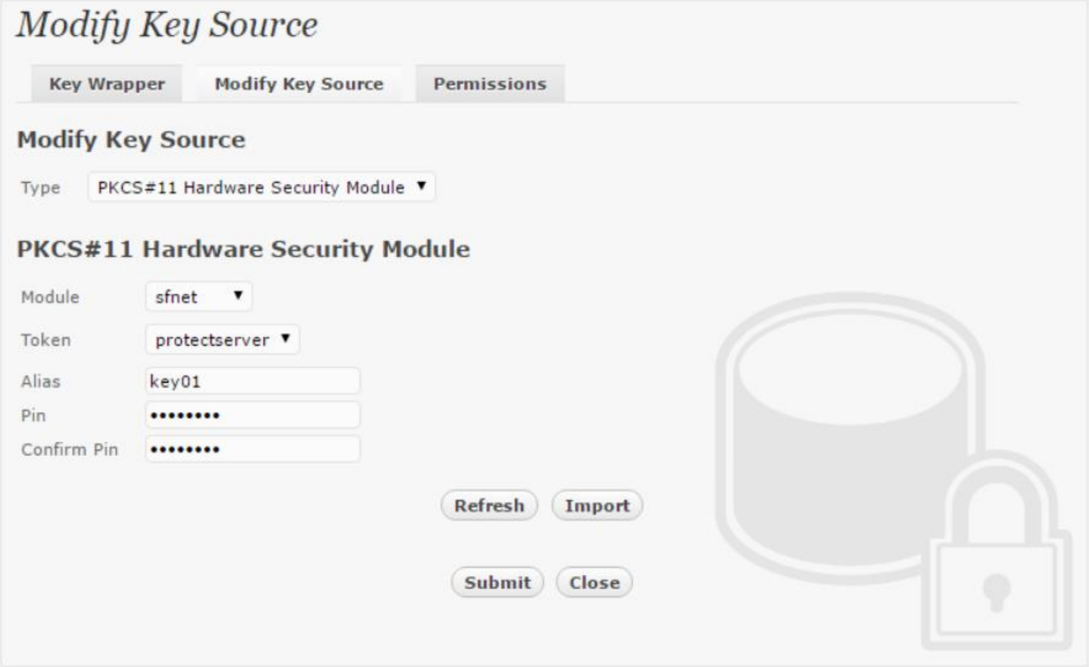
PKCS#11 Hardware Security Module

Module sfnet

Token protectserver

Key key01

And input the user pin of the token before submit the key wrapper.



Modify Key Source

Type PKCS#11 Hardware Security Module

PKCS#11 Hardware Security Module

Module sfnet

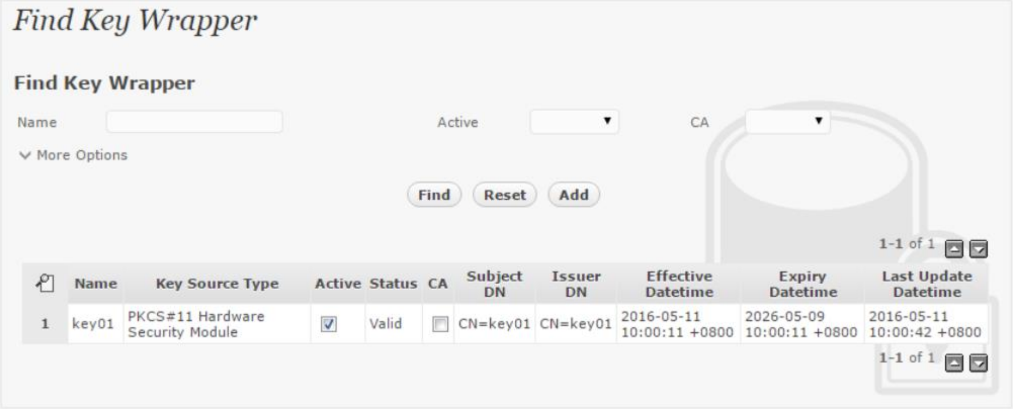
Token protectserver

Alias key01

Pin ••••••••

Confirm Pin ••••••••

The encryption key is now generated.



Find Key Wrapper

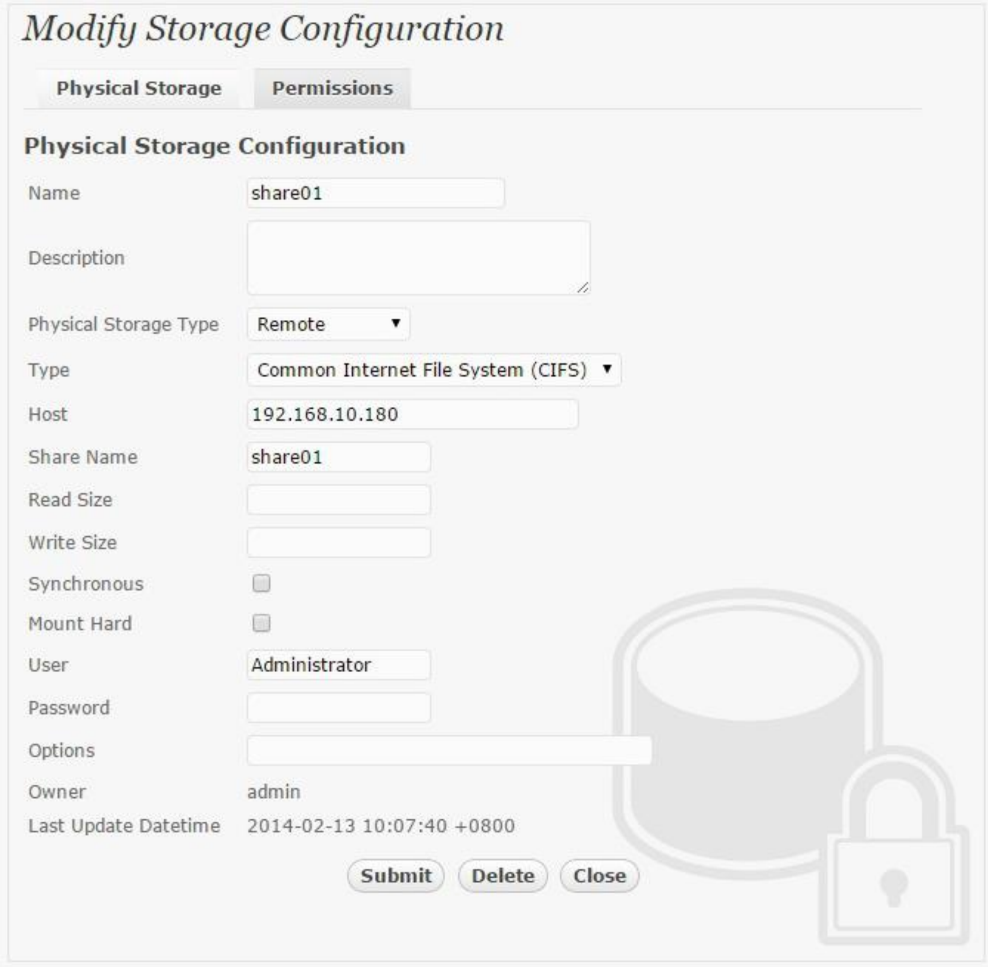
Find Key Wrapper

Name		Active	▾	CA	▾

	Name	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1	key01	PKCS#11 Hardware Security Module	☑	Valid	□	CN=key01	CN=key01	2016-05-11 10:00:11 +0800	2026-05-09 10:00:11 +0800	2016-05-11 10:00:42 +0800

Backend Physical Storage Configuration

Physical storage namely ‘share01’ is configured to be secured by Bloombase StoreSafe using encryption.



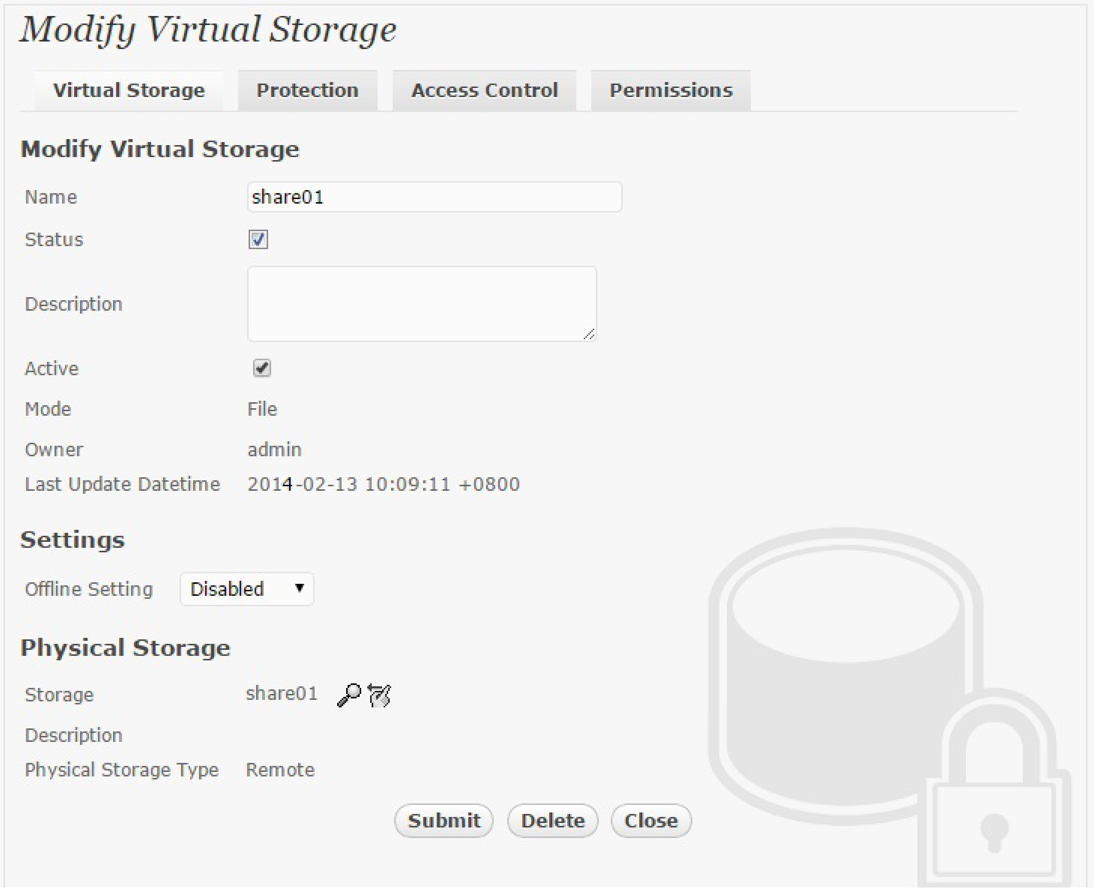
Modify Storage Configuration

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

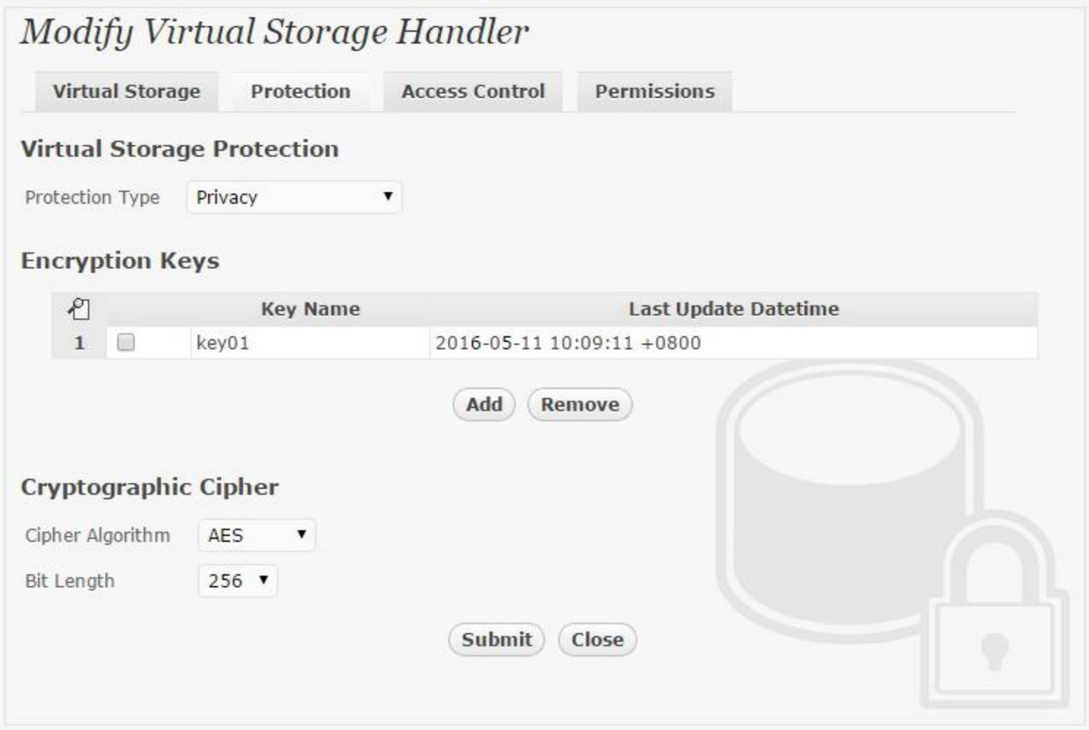
Settings

Offline Setting	Disabled ▾

Physical Storage

Storage	share01
Description	
Physical Storage Type	Remote

Protection type is specified as 'Privacy' and secure the backend EMC VNX storage using AES 256-bit encryption and encryption key 'key01' managed at Gemalto SafeNet ProtectServer.



Virtual Storage Protection

Protection Type: Privacy

Encryption Keys

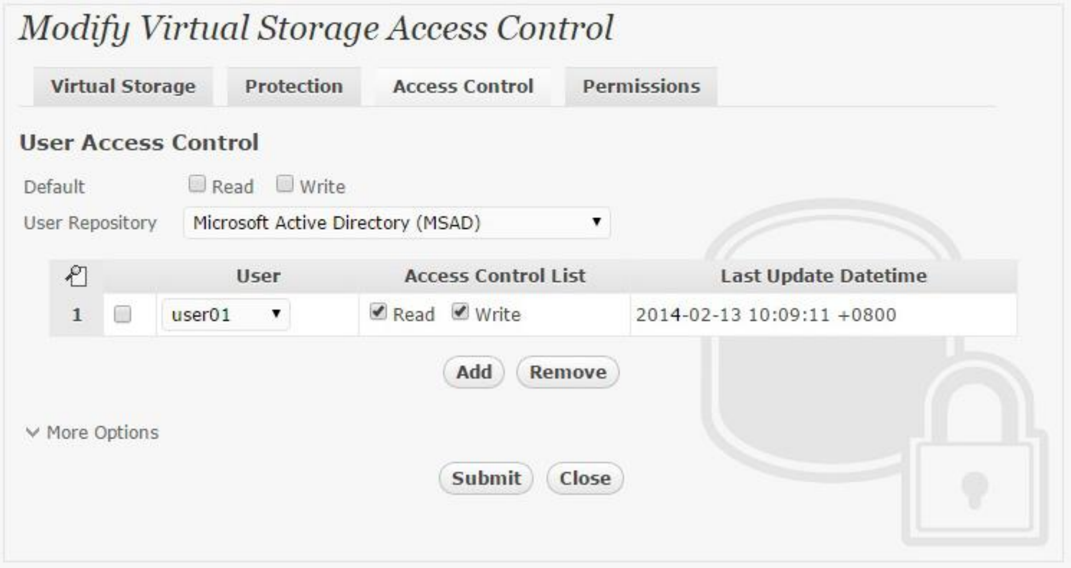
		Key Name	Last Update Datetime
1	□	key01	2016-05-11 10:09:11 +0800

Cryptographic Cipher

Cipher Algorithm: AES

Bit Length: 256

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.



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

Conclusion

Hardware security module

- Gemalto SafeNet ProtectServer

passed all Bloombase interopLab's interoperability tests with Bloombase StoreSafe

Bloombase Product	Operating System	Hardware Security Module
Bloombase StoreSafe	Microsoft Windows Server	• Gemalto SafeNet ProtectServer
	Red Hat Enterprise Linux (RHEL)	• Gemalto SafeNet ProtectServer
	SUSE Linux Enterprise Server (SLES)	• Gemalto SafeNet ProtectServer
	Oracle Solaris	• Gemalto SafeNet ProtectServer
	IBM AIX	• Gemalto SafeNet ProtectServer
	HP-UX	• Gemalto SafeNet ProtectServer

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.

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. Gemalto SafeNet ProtectServer, http://www.safenet-inc.com/data-encryption/hardware-security-modules-hsms/protectserver-security-module/