



Interoperability of Bloombase StoreSafe and Gemalto SafeNet Network HSM / Luna SA / AWS CloudHSM for Data-at-Rest Encryption

January 2017



Executive Summary

Gemalto SafeNet Network HSM Hardware Security Module (HSM) / AWS CloudHSM 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 Network HSM / AWS CloudHSM with Bloombase StoreSafe compute instance on Amazon EC2. Client host systems Microsoft Windows Server and Red Hat Enterprise Linux (RHEL) on AWS EC2 are tested with Gemalto SafeNet Network HSM / AWS CloudHSM and Bloombase StoreSafe for AWS EC2 with Amazon Elastic File System (Amazon EFS) 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.

© 2017 Bloombase, Inc.

Bloombase, Keyparc, Spitfire, StoreSafe are either registered trademarks or trademarks of Bloombase, Inc. in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Document No.: BLBS-TN-Bloombase-StoreSafe-Gemalto-SafeNet-Network-HSM-Luna-SA-AWS-CloudHSM-Interoperability-USLET-EN-Ro.92

Table of Contents

Table of Contents	3
Purpose and Scope	5
Assumptions	6
Infrastructure	7
Setup	7
Hardware Security Module	9
Bloombase StoreSafe	9
Storage System	9
Client Hosts	9
Configuration Overview	10
Gemalto SafeNet Network HSM / AWS CloudHSM	10
Initialization of the Network HSM / CloudHSM	11
Network Trust Link between StoreSafe and Network HSM / CloudHSM	11
Create and assign partition to Bloombase Storesafe	11
Key Generation in Network HSM	12
Amazon Elastic File System (EFS) Storage	13
Bloombase StoreSafe	14
Network Security, Trust and Authentication Configuration	14
Gemalto SafeNet Network HSM / AWS CloudHSM and Bloombase KeyCastle Integration	15
Encryption Key Provisioning	16
Backend Physical Storage Configuration	19
Secure Storage Configuration	20
Conclusion	22
Disclaimer	23
Technical Reference	24

Purpose and Scope

This document describes the steps necessary to integrate Gemalto SafeNet Network HSM (formerly Luna SA) Hardware Security Module (HSM) / AWS CloudHSM with Bloomberg StoreSafe to secure sensitive enterprise business data-at-rest managed in storage systems. Specifically, we cover the following topics:

- Install and configure Bloomberg StoreSafe Amazon EC2 Compute Instance
- Integrate Bloomberg StoreSafe with Gemalto SafeNet Network HSM (formerly Luna SA) / AWS CloudHSM
- Interoperability testing on client host compute instances on Amazon EC2 including Linux and Windows

Assumptions

This document describes interoperability testing of Gemalto SafeNet Network HSM (formerly SafeNet Luna SA) and AWS CloudHSM Hardware Security Module (HSM) with Bloombase StoreSafe. Therefore, it is assumed that the reader is familiar with operation of Gemalto SafeNet Network HSM / AWS CloudHSM, storage systems and major operating systems including Linux and Microsoft Windows. 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.

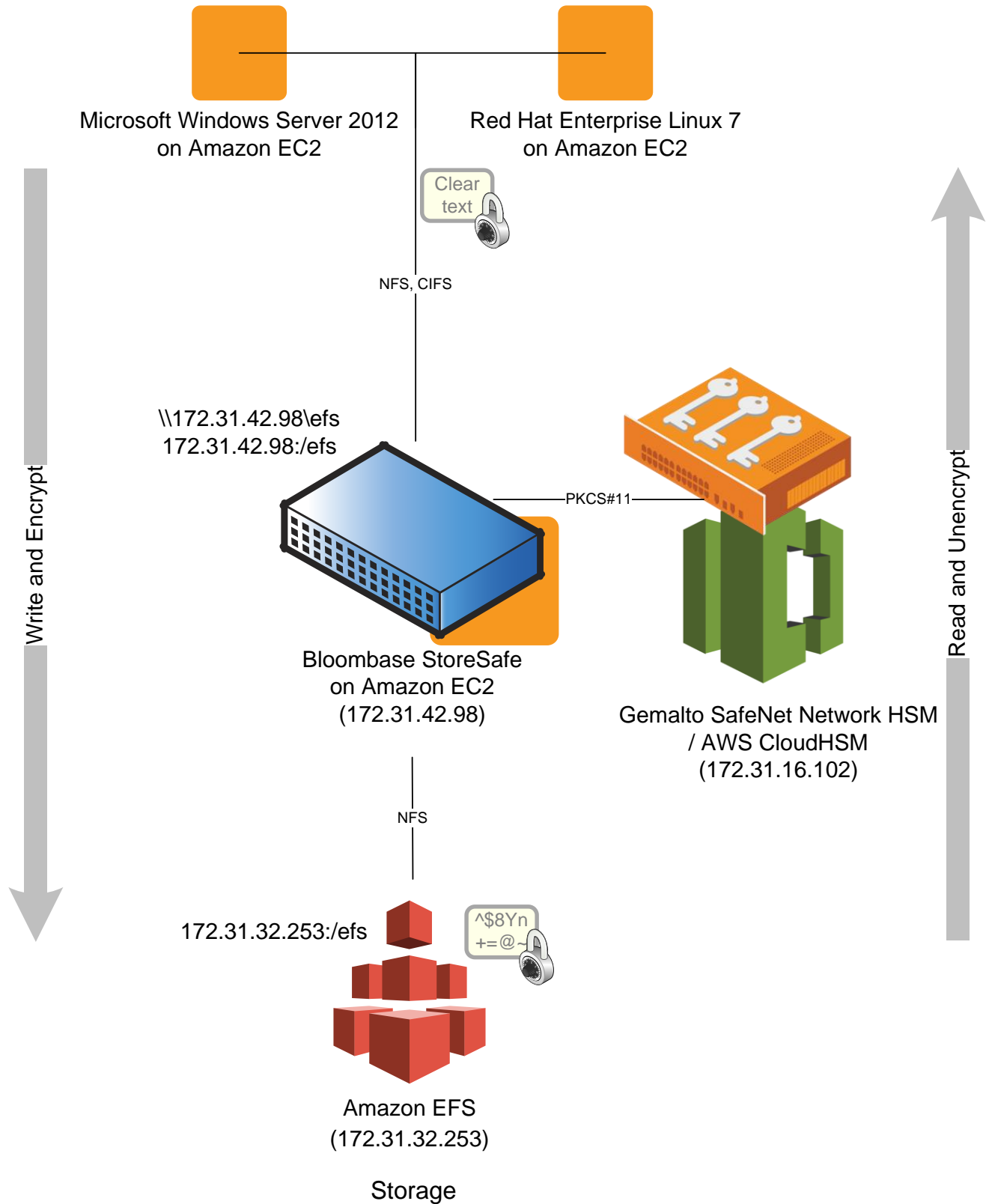
As Gemalto SafeNet Network HSM and AWS CloudHSM is a third party hardware option to Bloombase StoreSafe data-at-rest encryption security solution, the reader is recommended to refer to installation and configuration guides of specific model of Gemalto SafeNet Network HSM / AWS CloudHSM for the actual 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



Hardware Security Module

Hardware Security Module	Gemalto SafeNet Network HSM / AWS CloudHSM Luna K6
--------------------------	--

Bloombase StoreSafe

Bloombase StoreSafe	Bloombase StoreSafe Compute Instance v3.5 on AWS EC2
Processor	1 x Virtual CPU (vCPU)
Memory	4 GB

Storage System

Storage System	Amazon Elastic File System (EFS)
----------------	----------------------------------

Client Hosts

Operating System	Microsoft Windows Server 2012 on Amazon EC2	Red Hat Enterprise Linux 7 on Amazon EC2
------------------	---	--

Configuration Overview

Gemalto SafeNet Network HSM / AWS CloudHSM

Gemalto SafeNet Network Hardware Security Modules (HSMs) / AWS CloudHSM are designed to protect cryptographic keys against compromise while providing encryption, signing and authentication services to secure Java and sensitive web applications.

Gemalto SafeNet Network HSMs /AWS CloudHSM 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 Network HSM /AWS CloudHSM are used by Bloombase StoreSafe for encryption protection of data-at-rest for general-purpose use cases.

Gemalto SafeNet Network HSM /AWS CloudHSM is setup and configured as a network attached appliance with IP address 172.31.16.102 and with certification / public key installed to allow client connection through SSH.

Luna Client Software is properly installed on Bloombase Storesafe compute instance and with SSH private key installed to establish remote connection to Network HSM / CloudHSM via SSH.

Initialization of the Network HSM / CloudHSM

Connect to the Network HSM via local serial link or SSH (SSH private key will be needed), login as 'admin' with initial password 'PASSWORD' (or as 'manager' with CloudHSM). Then initialize the Network HSM with following command:

```
lunash:> hsm -init -label <label_for_network_hsm>
```

Followed by inputting password for security officer (SO), cloning domain.

Network Trust Link between StoreSafe and Network HSM / CloudHSM

First import the HSM Appliance Server certificate 'server.pem' from the Network HSM / Cloud HSM appliance to the SafeNet HSM client workstation and then register it

```
scp -i ~/.ssh/ssh_private_key admin@172.31.16.102:server.pem /usr/safenet/lunaclient/cert/server/  
/usr/safenet/lunaclient/bin/vtl addServer -n 172.31.16.102 -c server.pem
```

Then create a certificate and private key for the client, and export to the HSM appliance

```
/usr/safenet/lunaclient/bin/vtl createcert -n storesafe  
scp -i ~/.ssh/ssh_private_key /usr/safenet/lunaclient/cert/client/storesafe.pem admin@172.31.16.102:
```

Connect to the Network HSM appliance, login as SO and register 'storesafe' as client

```
lunash:> hsm login  
  
lunash:> client register -client storesafe -hostname storesafe
```

Create and assign partition to Bloombase Storesafe

Login to Network HSM as SO, then create partition and assign 'storesafe' to it

```
lunash:> hsm login  
  
lunash:> partition create -partition networkhsm  
  
lunash:> client assignPartition -client storesafe -partition networkhsm
```

Key Generation in Network HSM

Deploy Luna Client Software package at the client workstation to be used by Java Keytool for key generation via the Luna API

```
cp -p /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar $JAVA_HOME/jre/lib/ext/  
cp -p /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so $JAVA_HOME/jre/lib/ext/
```

Edit file `$JAVA_HOME/jre/lib/security/java.security` to include the Luna security provider

```
security.provider.3=com.safenetinc.luna.provider.LunaProvider
```

Create a keystore file `/etc/luna.keystore` with only one line of content to specify the HSM partition

```
tokenlabel:networkhsm
```

Then generate an asymmetric key pair using Java Keytool to be used for data-at-rest encryption at Bloombase StoreSafe

```
keytool -genkeypair -alias luna_key -keyalg RSA -keysize 2048 -keystore /etc/luna.keystore -storetype  
Luna
```

Alternatively, users can utilize Java Keytool to import PKCS#12 key file into Network HSM / CloudHSM through Client Tool 'CMU'

Amazon Elastic File System (EFS) Storage

Amazon Elastic File System (EFS) is used in this interoperability testing as backend storage service in which files are to be encrypted by Bloombase StoreSafe using keys from AWS CloudHSM.

Amazon EFS is accessible using Network File System (NFS) protocol.

File systems

Create file systemActions

	Name	File system ID	Metered size	Number of mount targets	Creation date
<div><div></div><div></div></div>		fs-4d18d9e4	6.0 KiB	3	2016-12-14T18:30:56Z
<div><div></div><div></div></div>		fs-e3ab694a	64.0 KiB	3	2017-01-06T04:45:50Z

Other details

TagsManage tags

Owner ID

437061541627

Life cycle state

Available

Performance mode

General Purpose

No tags added

File system access

Manage file system access

DNS name

fs-e3ab694a.efs.us-west-2.amazonaws.com

Amazon EC2 mount instructions

AWS Direct Connect mount instructions

Mount targets

VPC	Availability Zone	Subnet	IP address	Mount target ID	Network interface ID	Security groups	Life cycle state
	us-west-2a	subnet-6a188201 (default)	172.31.22.106	fsmt-529a56fb	eni-81da61c2	sg-f24f878a - Wide Open	Available
vpc-941b81ff (default)	us-west-2b	subnet-6b188200 (default)	172.31.32.253	fsmt-559a56fc	eni-28888d59	sg-f24f878a - Wide Open	Available
	us-west-2c	subnet-69188202 (default)	172.31.4.51	fsmt-549a56fd	eni-41491011	sg-acb146c3 - default	Available

NFS storage resources are provisioned on Amazon EFS to be used in this testing.

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 Network HSM / AWS CloudHSM.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm	Public DNS (IPv4)	IPv4 Public IP	IPv6	Key Name	Monitoring
KL Bloombase Storesafe ...	i-0c6dc816159c9308d	t2.micro	us-west-2b	running	2/2 checks ...	N...	ec2-35-167-61-234.us-...	35.167.61.234	-	kl-awskeypair	disabled

Instance: i-0c6dc816159c9308d (KL Bloombase Storesafe EFS Interop)

Public DNS: ec2-35-167-61-234.us-west-2.compute.amazonaws.com

Description

Status Checks

Monitoring

Tags

Instance ID

i-0c6dc816159c9308d

Public DNS (IPv4)

ec2-35-167-61-234.us-west-2.compute.amazonaws.com

Instance state

running

IPv4 Public IP

35.167.61.234

Instance type

t2.micro

IPv6 IPs

-

Elastic IPs

Private DNS

ip-172-31-42-98.us-west-2.compute.internal

Availability zone

us-west-2b

Private IPs

172.31.42.98

Security groups

[launch-wizard-3](#), [view inbound rules](#)

Secondary private IPs

Scheduled events

No scheduled events

VPC ID

vpc-941b81ff

AMI ID

storesafe_el7 (ami-5b1ba93b)

Subnet ID

subnet-6b188200

Platform

-

Network interfaces

eth0

IAM role

-

Source/dest. check

True

Key pair name

kl-awskeypair

EBS-optimized

False

Owner

437061541627

Root device type

ebs

Launch time

January 12, 2017 at 3:42:02 PM UTC+8 (355 hours)

Root device

/dev/sda1

Termination protection

False

Block devices

/dev/sda1

Lifecycle

normal

Monitoring

basic

Alarm status

None

Kernel ID

-

RAM disk ID

-

Placement group

-

Virtualization

hvm

Reservation

r-030783fa8b1eb0e2f

AMI launch index

0

Tenancy

default

Host ID

-

Affinity

-

State transition reason

-

Bloombase StoreSafe software appliance is deployed as an EC2 compute Instance on Amazon Web Services.

Network Security, Trust and Authentication Configuration

In this interoperability test effort, Bloombase StoreSafe serves as the client of Gemalto SafeNet Network HSM / AWS CloudHSM for encryption key access to deliver data at-rest encryption services. Authentication of Bloombase StoreSafe to the Gemalto SafeNet Network HSM / Amazon CloudHSM is established through the specification of passphrase.

Gemalto SafeNet Network HSM / AWS CloudHSM and Bloombase KeyCastle Integration

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

Modify Hardware Security Module

Modify Hardware Security Module

Module

Label

Pin

Confirm Pin

In this scenario, use the Gemalto SafeNet Network HSM / AWS CloudHSM with a token label 'networkhsm' and user pin as Pin. When Gemalto SafeNet Network HSM / AWS CloudHSM 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	networkhsm	<input checked="" type="checkbox"/>	1	1	luna	Safenet, Inc.	LunaSA 5.3.13	510981027	0.0 / 6.202	<input checked="" type="checkbox"/>

Encryption Key Provisioning

Associate the CloudHSM / Luna encryption key with name 'luna_key' in bundled Bloombase KeyCastle key life-cycle management tool.

Modify Key Wrapper

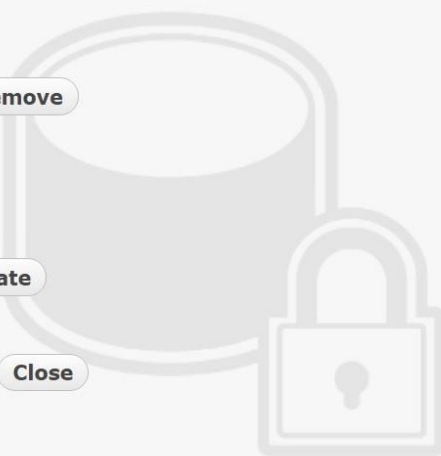
Key Wrapper Upload Key Contents Modify Key Source CRLDP OCSP Permissions

Modify Key Wrapper

Name	luna_key
Type	Asymmetric
Active	<input checked="" type="checkbox"/>
Exportable	<input type="checkbox"/>
Key Bit Length	2048 ▼
Signature Hash	SHA256 ▼
Key Usage	<input type="checkbox"/> Digital Signature
	<input type="checkbox"/> Non Repudiation
	<input type="checkbox"/> Key Encipherment
	<input type="checkbox"/> Data Encipherment
	<input type="checkbox"/> Key Agreement
	<input type="checkbox"/> Key Cert Sign
	<input type="checkbox"/> C R L Sign
	<input type="checkbox"/> Encipher Only
	<input type="checkbox"/> Decipher Only
	Extended Key Usage
Owner	admin
Last Update Datetime	

Generate

Submit Close



Click 'Modify Key Source' and select Key Source Type as 'PKCS#11 Hardware Security Module' with Module 'luna', assign HSM token label as 'networkhsm' and Key as 'luna_key'.

Modify Key Source

Key Wrapper **Modify Key Source** Permissions

Modify Key Source

Type

PKCS#11 Hardware Security Module

Module

Token

Key



Enter token passphrase

Modify Key Source

Key Wrapper **Modify Key Source** Permissions

Modify Key Source

Type

PKCS#11 Hardware Security Module

Module

Token

Alias

Pin

Confirm Pin



The newly provisioned encryption key setting now points to the key object managed at Network HSM.

*Find Key Wrapper***Find Key Wrapper**

Name Type Active CA

More Options

Find Reset Add

1-1 of 1

	Name	Type	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1	luna_key	Asymmetric	PKCS#11 Hardware Security Module	<input checked="" type="checkbox"/>	Valid	<input checked="" type="checkbox"/>	CN=Storesafe OU=Support O=Bloomberg L=Sunnyvale ST=CA C=US	CN=Storesafe OU=Support O=Bloomberg L=Sunnyvale ST=CA C=US	2017-01-25 01:00:25 -0500	2017-04-25 02:00:25 -0400	2017-01-25 01:32:56 -0500

1-1 of 1

Backend Physical Storage Configuration

Physical storage namely 'EFS' is configured to be secured by Bloomberg StoreSafe by strong encryption with keys managed at CloudHSM.

Modify Storage Configuration

Physical Storage

Permissions

Physical Storage Configuration

Name

Description

Physical Storage Type

Type

Host

Share Name

Read Size

Write Size

Synchronous ☐

Mount Hard ☐

Options

Virtual Storage

Owner

Last Update Datetime

Submit Delete Close

Secure Storage Configuration

Virtual storage namely 'EFS' of type 'File' is created to virtualize physical storage 'EFS' for application transparent encryption protection over network file protocols CIFS and NFS.

Modify Virtual Storage

Virtual Storage

Protection

Access Control

Permissions

Modify Virtual Storage

NameEFS

Status☒

Description

Active☒

ModeFileOwneradminLast Update Datetime2017-01-12 03:51:52 -0500

Settings

Offline SettingDisabled

Physical Storage

StorageEFS

Description

Physical Storage TypeRemote

Submit

Delete

Status

Close

Protection type is specified as 'Privacy'. Configure protection profile to secure the backend Amazon EFS using AES 256-bit encryption with encryption key 'luna_key' managed at Gemalto SafeNet Network HSM / AWS CloudHSM.

Modify Virtual Storage Handler

Virtual Storage

Protection

Access Control

Permissions

Virtual Storage Protection

Protection TypePrivacy

Encryption Keys

	Key Name	Last Update Datetime
1	luna_key	2017-01-25 01:50:29 -0500

Add

Remove

Cryptographic Cipher

Cipher AlgorithmAES

Bit Length256

Submit

Close

CIFS storage protocol relies mainly on user-password authentication for access control. In this test, the Bloombase StoreSafe secure storage resource ‘EFS’ is provisioned for user ‘user’ with for user-password authentication and single sign-on.

Modify Virtual Storage Access Control

Virtual Storage

Protection

Access Control

Permissions

User Access Control

Default

☐ Read

☐ Write

User Repository

Local

		User	Access Control List	Last Update Datetime
1	<input type="checkbox"/>	user	<div><div><input checked="" type="checkbox"/> Read</div><div><input checked="" type="checkbox"/> Write</div></div>	2017-01-25 01:50:29 -0500

Add

Remove

More Options

Refresh

Submit

Close

Conclusion

Hardware Security Module

- Gemalto SafeNet Network HSM (formerly Luna SA) / AWS CloudHSM

passed all Bloomberg interopLab's interoperability tests with Bloomberg StoreSafe

Bloomberg Product	Operating System	Hardware Security Module
Bloomberg StoreSafe	Microsoft Windows Server 2012	<ul style="list-style-type: none">• Gemalto SafeNet Network HSM (formerly Luna SA) / AWS CloudHSM
	Red Hat Enterprise Linux (RHEL) 7	<ul style="list-style-type: none">• Gemalto SafeNet Network HSM (formerly Luna SA) / AWS CloudHSM

Disclaimer

The tests described in this paper were conducted in the Bloomberg InteropLab. Bloomberg has not tested this configuration with all the combinations of hardware and software options available. There may be significant 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 Network HSM, <https://safenet.gemalto.com/data-encryption/hardware-security-modules-hsms/safenet-network-hsm/>
4. AWS CloudHSM, <https://aws.amazon.com/cloudhsm/>
5. AWS EC2, <https://aws.amazon.com/ec2/>
6. AWS EFS, <https://aws.amazon.com/efs/>