

interopLab

Interoperability of Bloombase StoreSafe and Utimaco CryptoServer for Data-at-Rest Encryption

April 2016

BLOOMBASE®

Executive Summary

Utimaco CryptoServer 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 Utimaco CryptoServer 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 Utimaco CryptoServer powered Bloombase StoreSafe with EMC VNX unified storage system as backend storage.

Document No.: BLBS-TN-Bloombase-StoreSafe-Utimaco-CryptoServer-Interoperability-USLET-EN-R0.94

Table of Contents

Purpose and Scope

This document describes the steps necessary to integrate Utimaco CryptoServer 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 Utimaco CryptoServer
- Interoperability testing on client host systems including Linux, Windows, IBM AIX, HP-UX and Oracle Sun Solaris

Assumptions

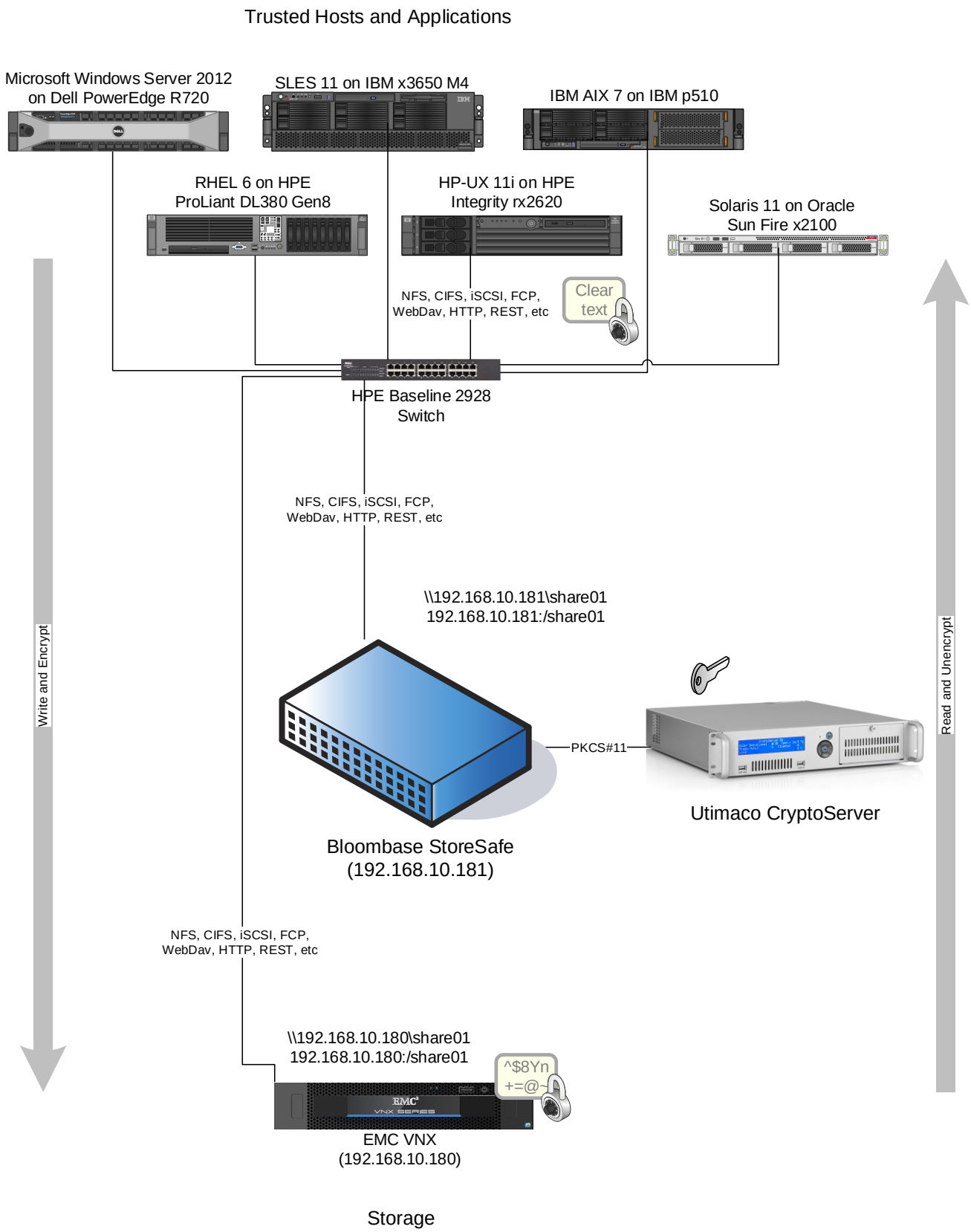
This document describes interoperability testing of Utimaco CryptoServer with Bloombase StoreSafe. Therefore, it is assumed that the reader is familiar with operation of Utimaco CryptoServer, storage systems and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun 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 Utimaco CryptoServer 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 Utimaco CryptoServer 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:



Utimaco Hardware Security Module

Hardware Security Module	Utimaco CryptoServer LAN

Bloombase StoreSafe

Bloombase StoreSafe	Bloombase StoreSafe Software Appliance v3.5 on Bloombase OS 7
CryptoServer Client Software Package	SecurityServer V4.00.0
Server	VMware Virtual Machine (VM) on VMware ESXi 5.5
Processor	4 x Virtual CPU (vCPU)
Memory	8 GB

Storage System

Storage System	EMC VNX Virtual Appliance on ESXi 5.5

Client Hosts

Model	Dell PowerEdge R720	HPE ProLiant DL380 Gen8	IBM System x3650 M4	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

Utimaco CryptoServer

Utimaco CryptoServer is a hardware security module that secures cryptographic key material for servers and applications. It includes integration software that supports the industry standards (e.g. PKCS#11, Microsoft CSP/CNG, JCE…) which are used in many application scenarios, e.g., Enterprise PKI application and database encryption. The CryptoServer is available as PCIe embedded card or as network attached appliance. The key management and cryptographic functionalities provided by Utimaco CryptoServer are used by Bloombase StoreSafe for encryption protection of data-at-rest for general-purpose use cases.

Utimaco CryptoServer Configurations

Assume Utimaco CryptoServer LAN is configured with IP 192.168.10.50 through the on-machine display and control buttons.

To configure Utimaco CryptoServer LAN, install the configuration softwares (`csadm` and `p11tool2`) on a computer, and connect the computer to the network of the Utimaco CryptoServer LAN. Here we assume a CentOS 7 machine is used.

The Utimaco CryptoServer HSM is supplied from the factory with a default ADMIN user, and provides a default key file ‘ADMIN.key’ for that user. The examples below may use the ADMIN user for authentication, but in a production environment, the factory ADMIN user will not exist, and the replacement administrator(s) are expected to be using personal PIN-protected smart cards for authentication. For information on how this will alter the example commands below in your production environment, refer to the Utimaco documentation – specifically, ‘csadm help=LogonSign’.

Configure Master Backup Key (MBK)

In order to provide backup functionality, Utimaco CryptoServer is able to store up to four Master Backup Keys (in slot 0...3) to be used by various applications. MBK of AES type must be stored in slot 3.

Generate a Master Backup Key (MBK) of AES type in an m-out-of-n scheme for the Utimaco CryptoServer using the following command.

```
csadm Dev=<IP> LogonSign=<AdminUser>,<Token> Key=<keyspec>
MBKGenerateKey=<keytype>,<keylength>[<n>,<m>,<keyname>]
```

As an example,

```
csadm Dev=192.168.10.50 LogonSign=ADMIN,ADMIN.key Key=mbk01#123456,mbk02#123456
MBKGenerateKey=AES,32,2,2,mbk
```

Then import the MBK into the Utimaco CryptoServer using the following command.

```
csadm Dev=<IP> LogonSign=<AdminUser>,<Token> Key=<keyspec> MBKImportKey=<slot_no>
```

As an example,

```
csadm Dev=192.168.10.50 LogonSign=ADMIN,ADMIN.key Key=mbk01#123456,mbk02#123456 MBKImportKey=3
```

Check that the MBK is available in your Utimaco CryptoServer with the following command.

```
csadm Dev=<IP> MBKListKeys
```

Configure PKCS#11

Utimaco CryptoServer needs further configurations before Bloombase StoreSafe can communicate with it through PKCS#11. For instance, a security officer (SO) has to be created for token initialization, and an authorized user has to be created to use the token. Bloombase StoreSafe can then communicate with Utimaco CryptoServer using the user account.

We first setup the PKCS11 environment variable as

```
export CS_PKCS11_R2_CFG=<path to cs_pkcs11_R2.cfg>
```

Edit `cs_pkcs11_R2.cfg` for the IP address of Utimaco CryptoServer and the slot number of the token to be initialized.

To setup an SO for token initialization of the specific slot with a unique token label, run the following command.

```
p11tool2 slot=<number> Label=<unique label name> Login=<AdminUser>,<Token> InitToken=<so pin>
```


As an example, the Utimaco CryptoServer HSM is assigned a token label namely ‘utimaco’ as follows

```
p11tool2 slot=0 Label=utimaco Login=ADMIN,ADMIN.key InitToken=12345678
```

To setup a user account, run the following command,

```
p11tool2 slot=<number> LoginSO=<so pin> InitPin=<user pin>
```

As an example,

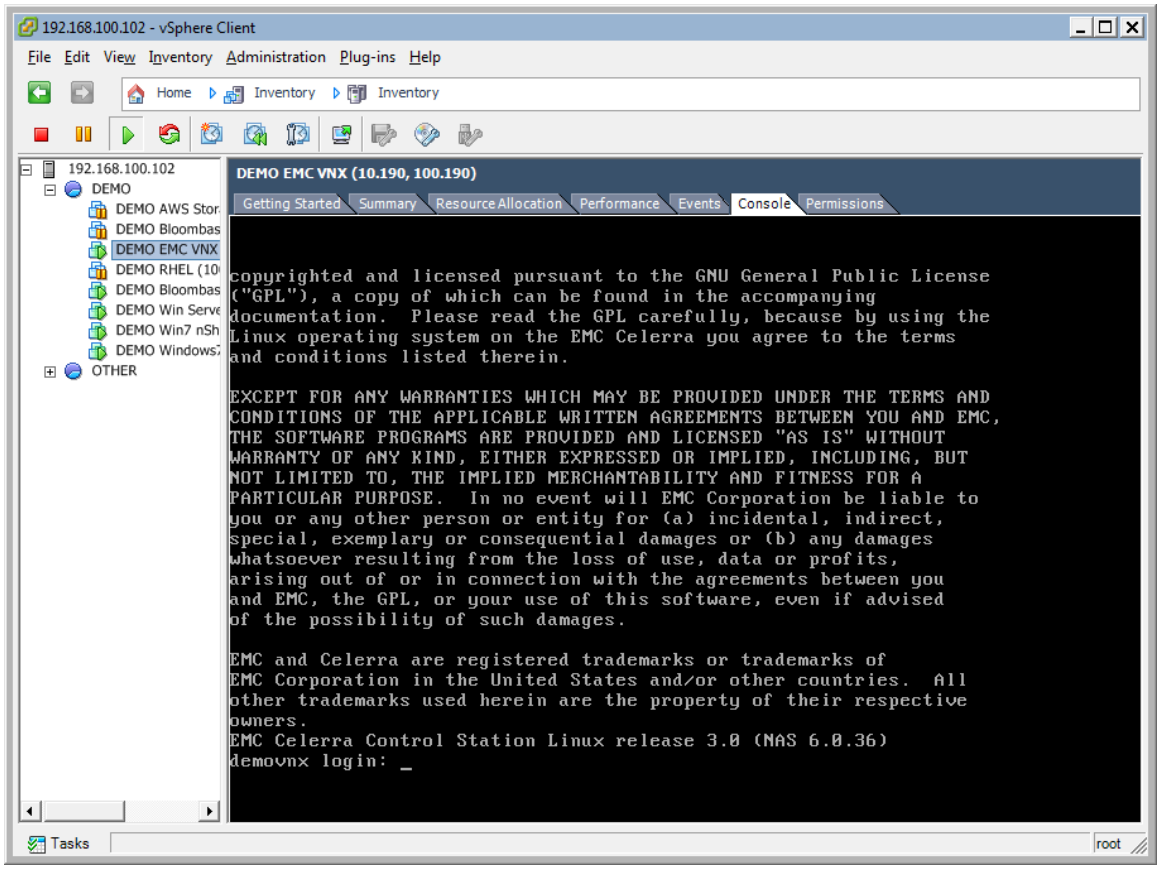
```
p11tool2 slot=0 LoginSO=12345678 InitPin=87654321
```

To check if Utimaco CryptoServer is properly setup, run

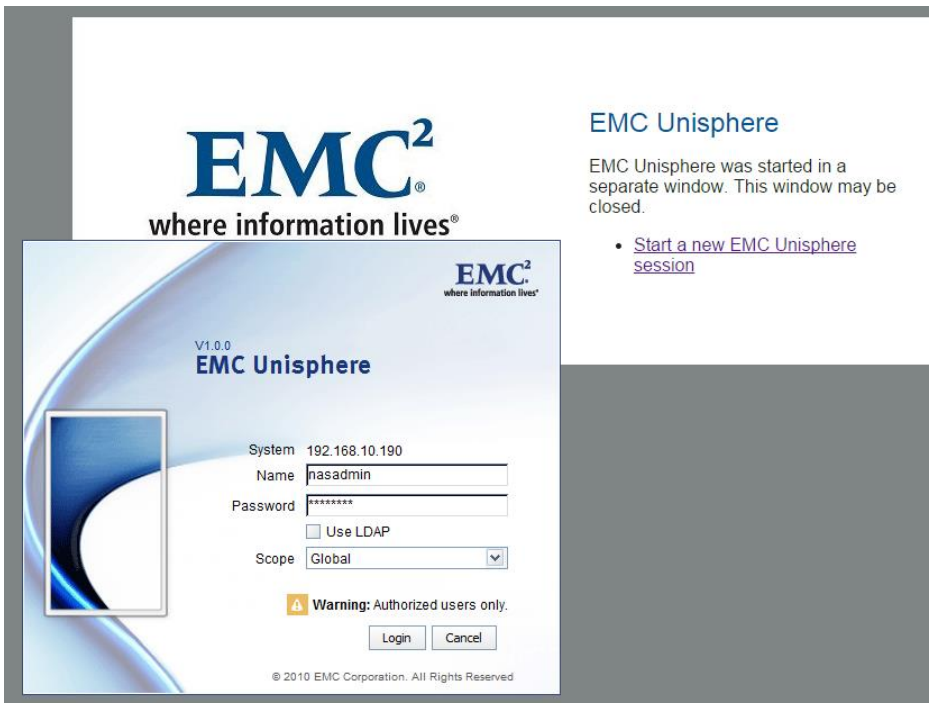
```
p11tool2 slot=0 GetTokenInfo

p11tool2 slot=0 GetSlotInfo

p11tool2 ListSlots=status
```


EMC VNX Storage

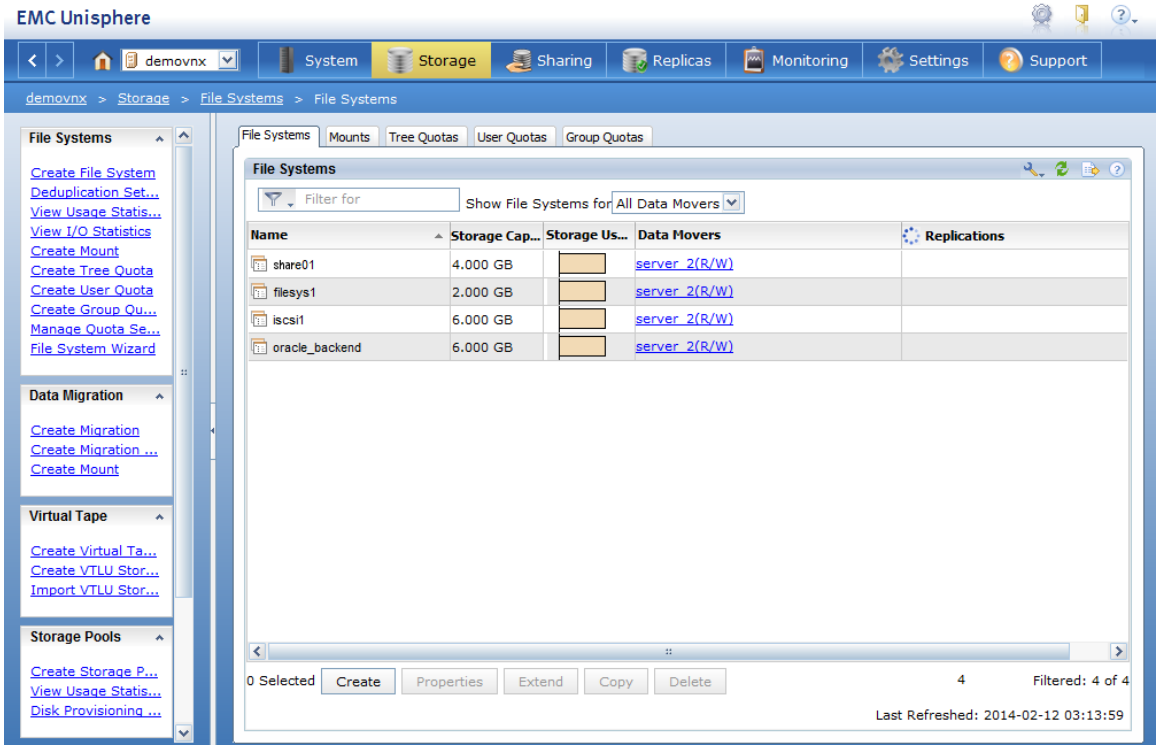
EMC VNX virtual appliance is used in this interoperability test which is able to provide storage services over network storage protocols including NFS, CIFS, iSCSI, etc.



EMC VNX is a unified storage system supporting multiple network storage protocols including NFS, CIFS, HTTP, FCP, FCoE, iSCSI, etc.

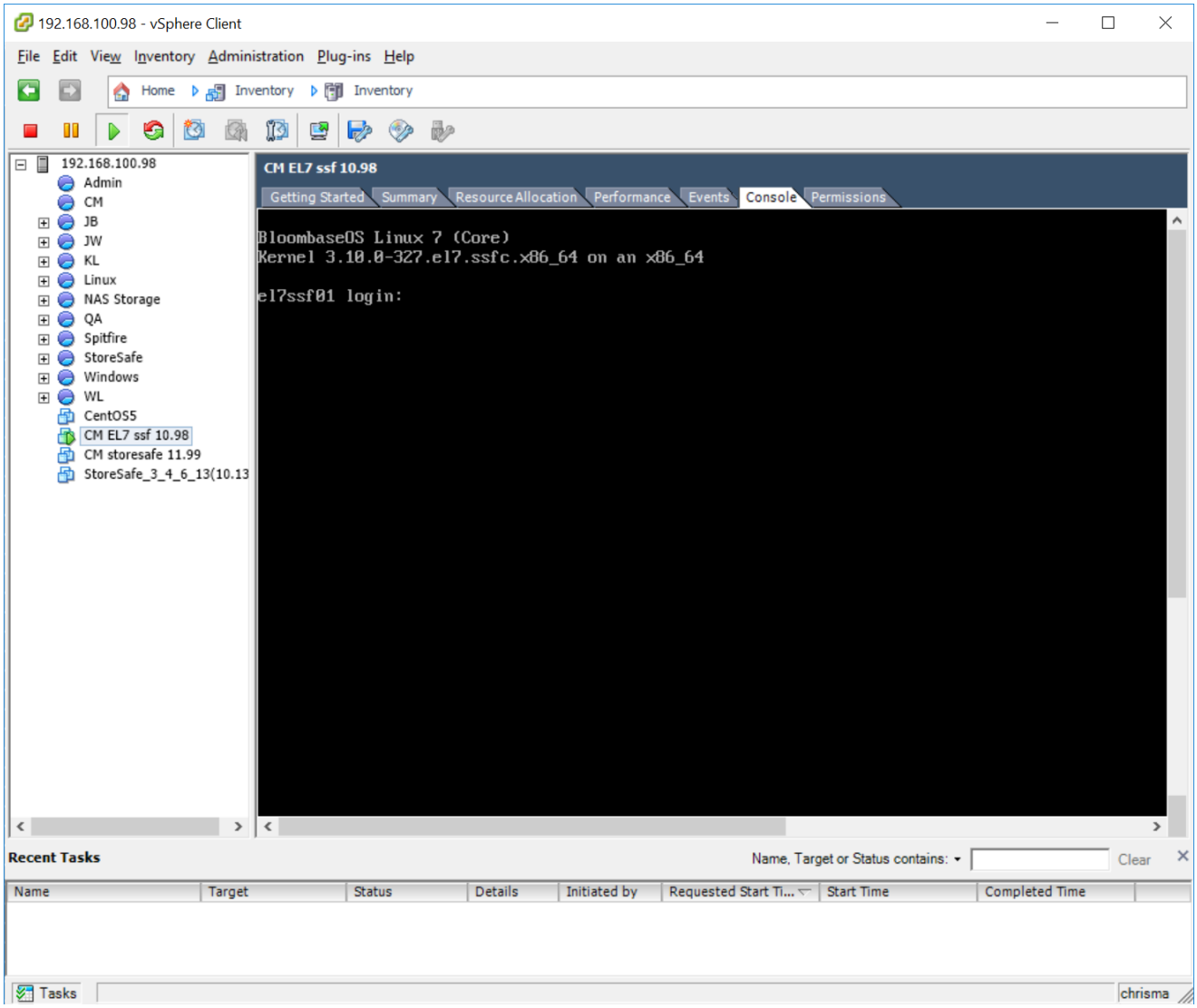


CIFS and NFS storage resources are provisioned on EMC VNX to be used in this testing.



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 Utimaco CryptoServer HSM.



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 Utimaco CryptoServer for encryption key access to deliver data at-rest encryption services. Authentication of Bloombase StoreSafe to the Utimaco CryptoServer through the specification of user pin.

Utimaco CryptoServer and Bloombase KeyCastle Integration

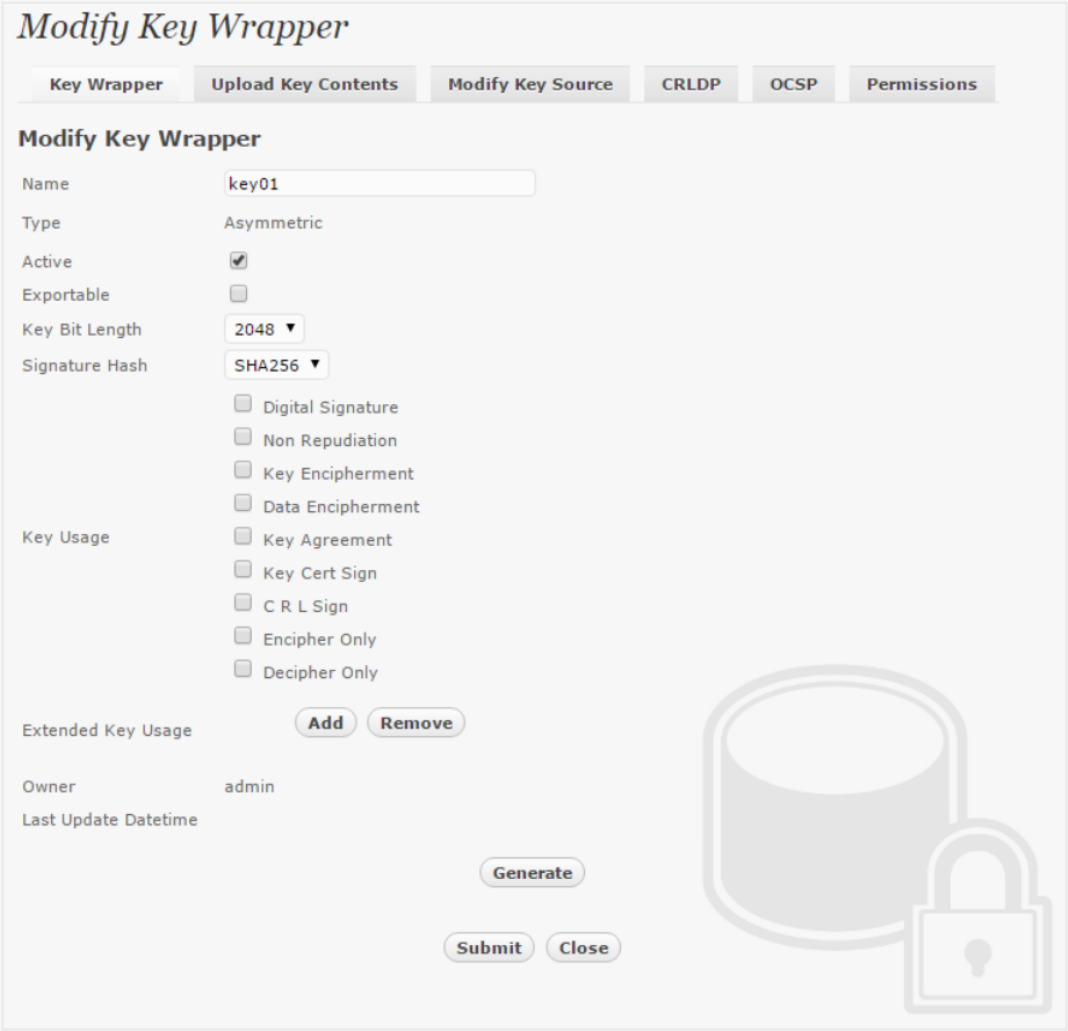
To configure Utimaco CryptoServer HSM at Bloombase web management console, select Module as 'utimaco' which allows the embedded Bloombase KeyCastle module to utilize Utimaco CryptoServer driver to access Utimaco CryptoServer over standard PKCS#11 protocol.

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

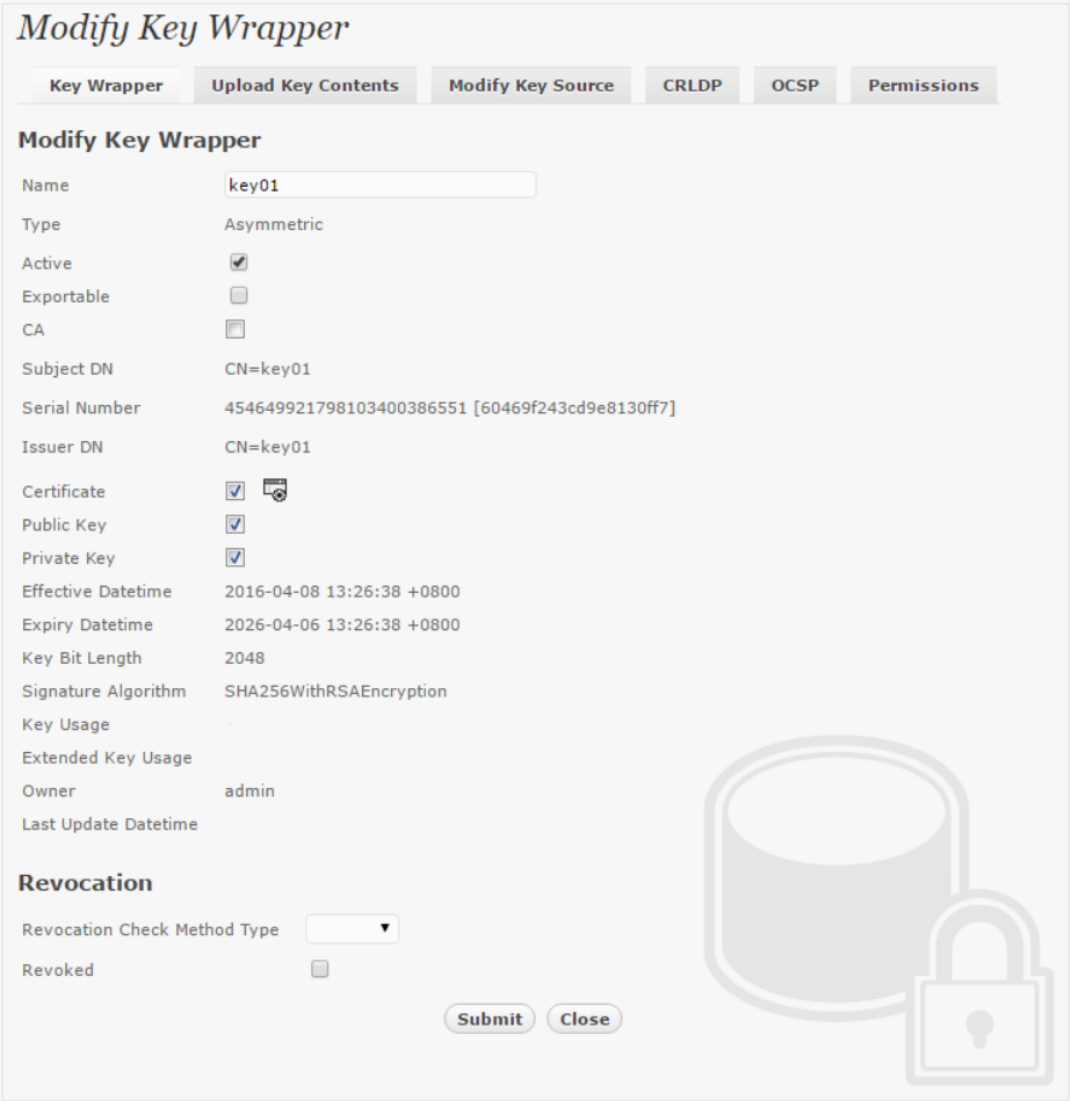
	Label	Present	Slot	Token	Module	Manufacturer	Model	Serial Number	Version	Status
1	utimaco	☑	0	0	utimaco	Utimaco IS GmbH	CryptoServer	UTIMACO CS000000	5.01 / 2.01	☑

Encryption Key Provisioning

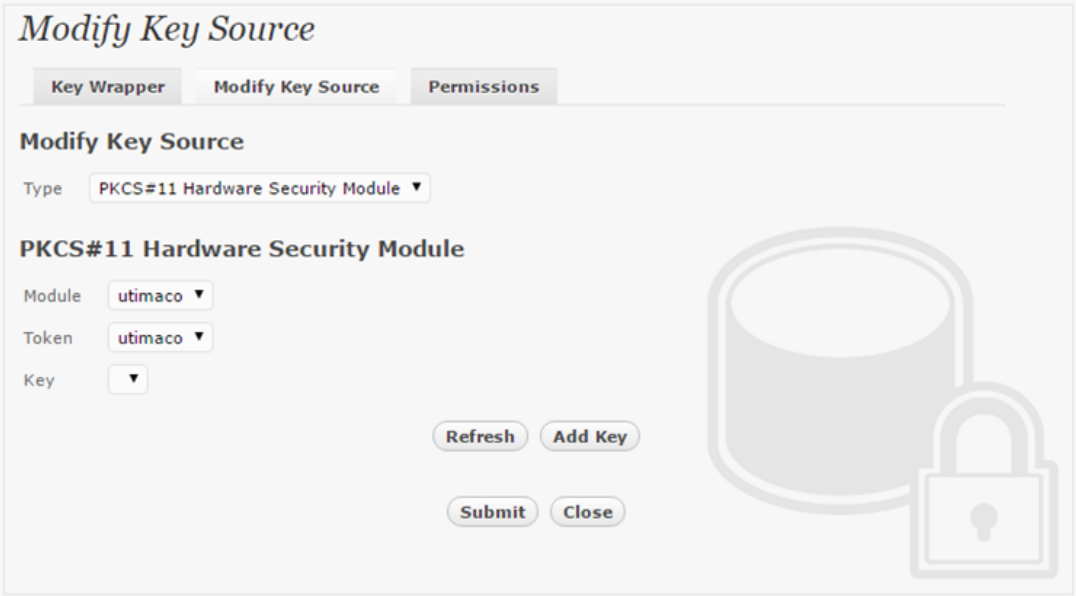
Generate encryption key with name 'key01' in bundled Bloombase KeyCastle key life-cycle management tool



To generate key in attached Utimaco CryptoServer HSM, input details of the key and click ‘Generate’.

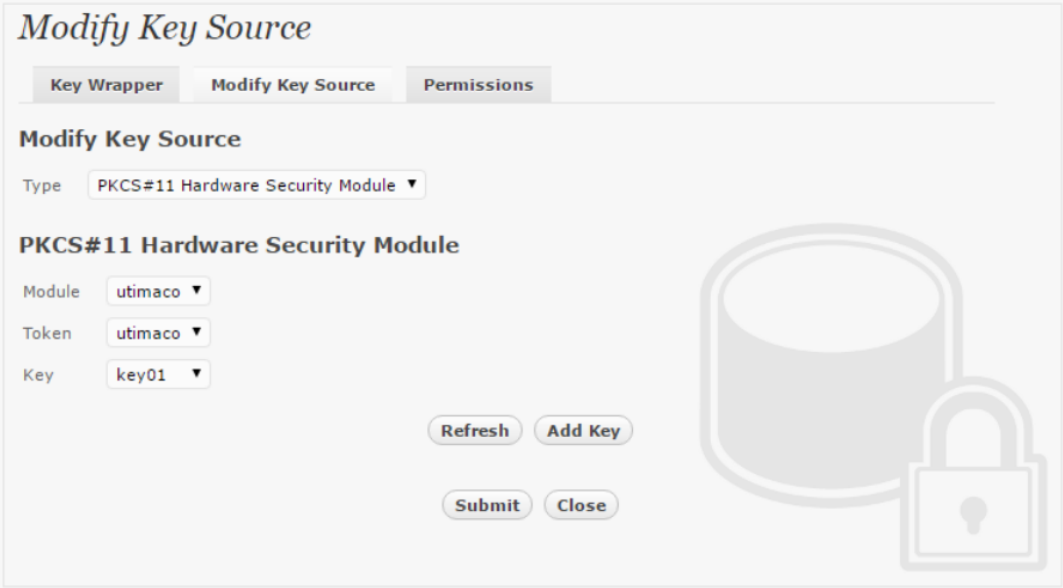


Then click 'Modify Key Source' and select Key Source Type as 'PKCS#11 Hardware Security Module', Module as 'utimaco' and the assigned HSM token label, in this case 'utimaco'.

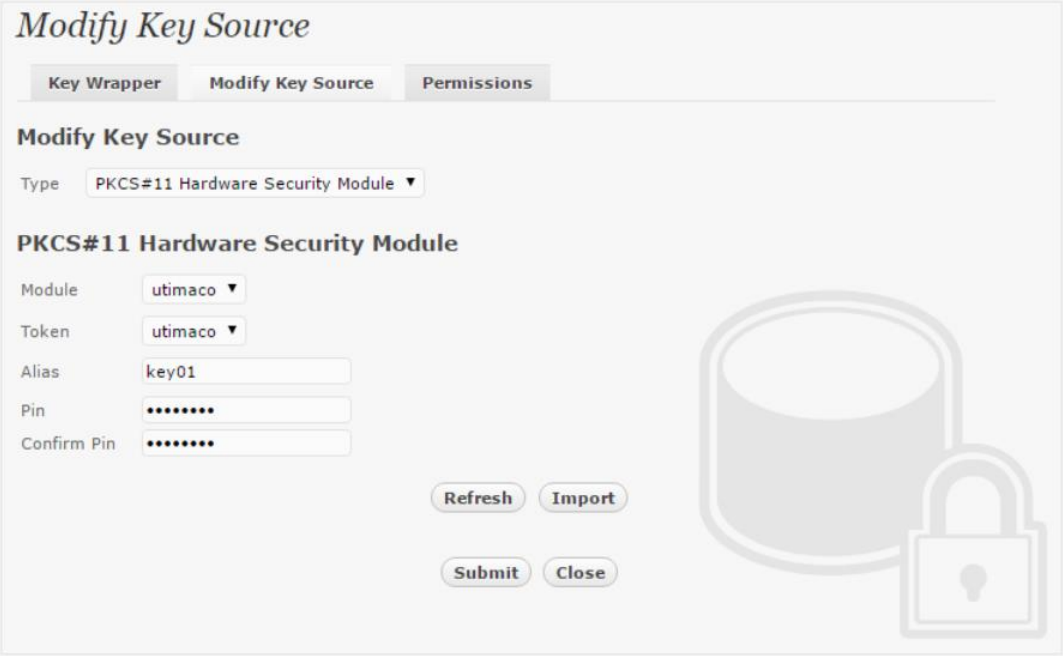


Select 'Add Key' to input a unique alias as the key name, and input the user pin of the token to import a new key from the HSM before you submit the key wrapper.

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



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



Backend Physical Storage Configuration

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

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.

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

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.

Conclusion

Hardware security module

- Utimaco CryptoServer LAN

passed all Bloombase interopLab's interoperability tests with Bloombase StoreSafe

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

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 Utimaco 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. Utimaco CryptoServer LAN, https://hsm.utimaco.com/cryptoserver/securityserver-se-2/