interopLab

Interoperability of Bloombase StoreSafe and Cavium LiquidSecurity HSM for Data-at-Rest Encryption

June 2018

BLOOMBASE®

Executive Summary

Cavium LiquidSecurity Hardware Security Module (HSM) is validated by Bloombase InteropLab as an integrated data-at-rest encryption solution with Bloombase StoreSafe. This document describes the steps carried out to test interoperability of Cavium LiquidSecurity HSM with Bloombase StoreSafe software appliance deployed on VMware vSphere / 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 the Bloombase StoreSafe data-at-rest encryption solution and secure key management at Cavium LiquidSecurity HSM for protection of data managed at Dell EMC VNX unified storage system.

Document No.: BLBS-TN-Bloombase-StoreSafe-Cavium-LiquidSecurity-HSM-Interoperability-USLET-EN-R0.97

Table of Contents

Purpose and Scope

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

Assumptions

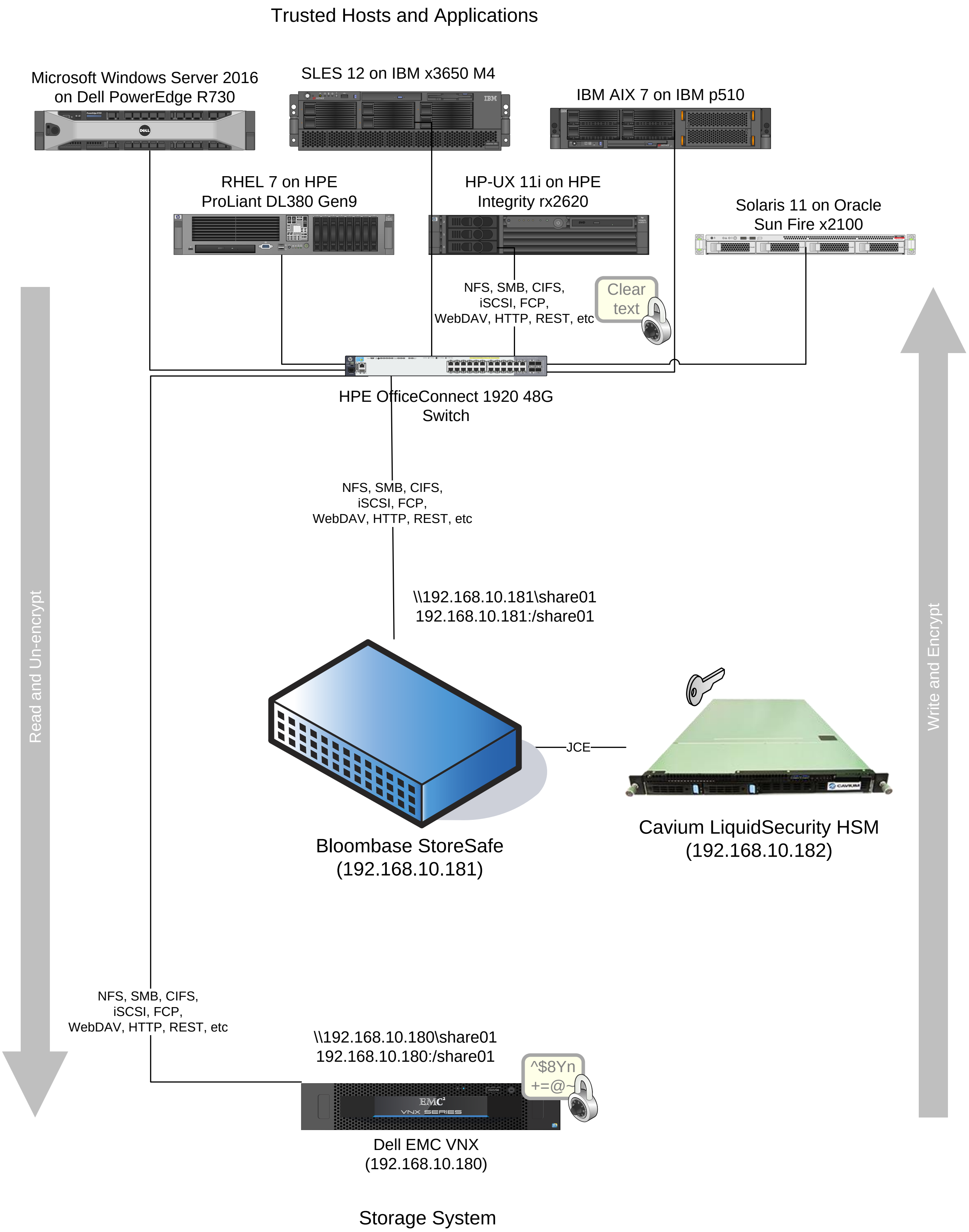
This document describes interoperability testing of Cavium LiquidSecurity Hardware Security Module (HSM) with Bloombase StoreSafe. Therefore, it is assumed that the reader is familiar with operation of Cavium LiquidSecurity HSM, storage systems and major operating systems including Linux, Microsoft Windows, 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 Cavium LiquidSecurity HSM is a third party option to the Bloombase StoreSafe data-at-rest encryption security solution, the reader is recommended to refer to installation and configuration guides of specific model and version of Cavium LiquidSecurity 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 https://www.bloombase.com and Bloombase SupPortal https://supportal.bloombase.com.

Testing Infrastructure

Setup

The testing environment is set up as in diagram below.


Trusted Hosts and Applications
Microsoft Windows Server 2016 on Dell PowerEdge R730
SLES 12 on IBM x3650 M4
IBM AIX 7 on IBM p510
RHEL 7 on HPE ProLiant DL380 Gen9
HP-UX 11i on HPE Integrity rx2620
Solaris 11 on Oracle Sun Fire x2100
NFS, SMB, CIFS, iSCSI, FCP, WebDAV, HTTP, REST, etc
Clear text
HPE OfficeConnect 1920 48G Switch
NFS, SMB, CIFS, iSCSI, FCP, WebDAV, HTTP, REST, etc
\\192.168.10.181\share01
192.168.10.181:/share01
Read and Un-encrypt
Write and Encrypt
JCE
Bloombase StoreSafe (192.168.10.181)
Cavium LiquidSecurity HSM (192.168.10.182)
NFS, SMB, CIFS, iSCSI, FCP, WebDAV, HTTP, REST, etc
\\192.168.10.180\share01
192.168.10.180:/share01
^$8Yn +=@~
Dell EMC VNX (192.168.10.180)
Storage System

Hardware Security Module

Hardware Security Module	Cavium LiquidSecurity HSM
IP Address	192.168.10.182

Bloombase StoreSafe

Bloombase StoreSafe	Bloombase StoreSafe Software Appliance 3.4
Server	VMware Virtual Machine (VM) on VMware vSphere 6.5
Processor	4 x Virtual CPU (vCPU)
Memory	8 GB
IP Address	192.168.10.181

Storage System

Storage System	Dell EMC VNX virtual appliance on VMware vSphere 6.5
IP Address	192.168.10.180

Client Hosts

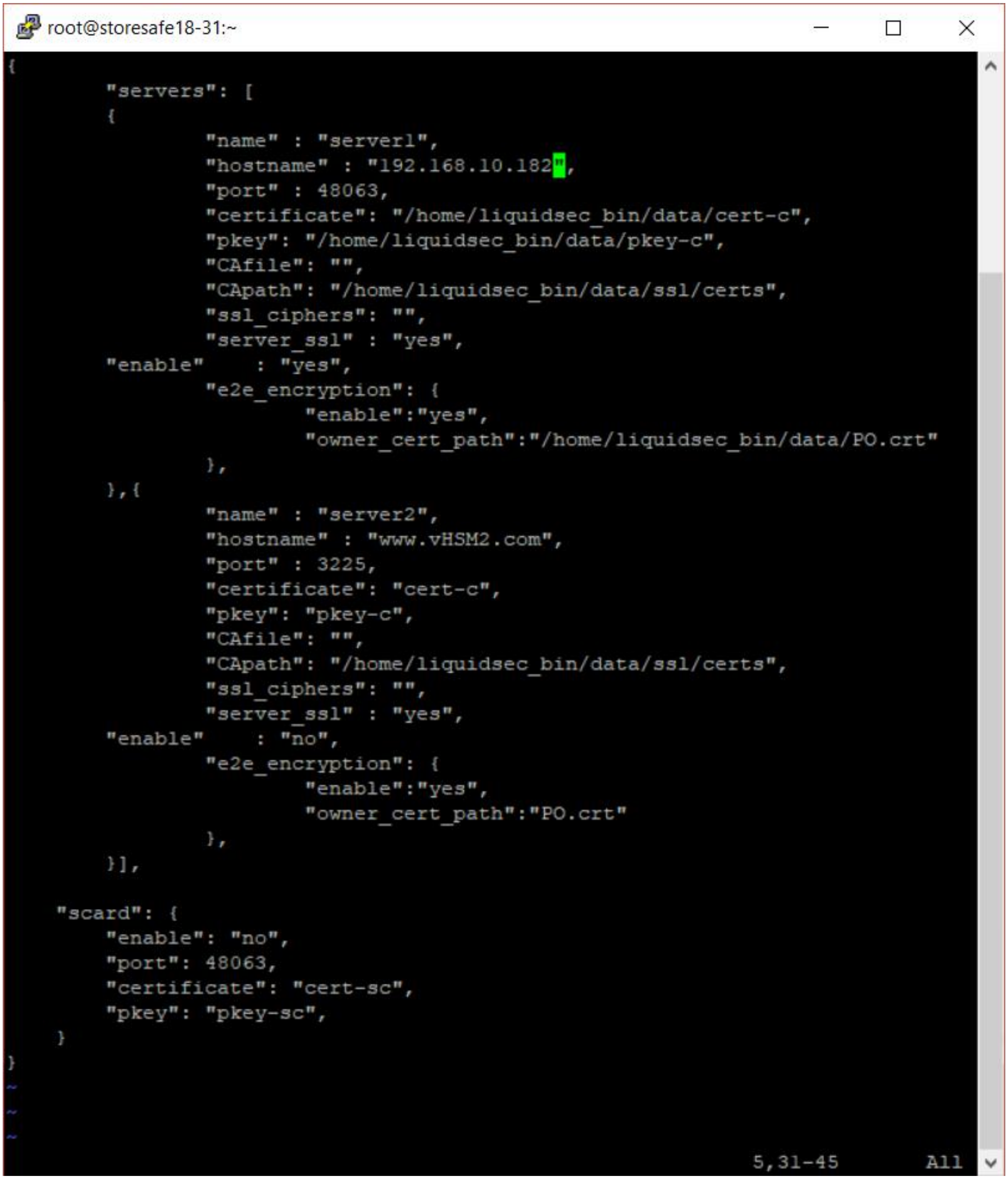
Server	Dell PowerEdge R730	HPE ProLiant DL380 Gen9	IBM System x3650 M4	HPE Integrity rx2620	IBM System p5 510	Oracle Sun Fire x2100
Operating System	Microsoft Windows Server 2016	Red Hat Enterprise Linux 7	SUSE Linux Enterprise 11	HP-UX 11i	IBM AIX 7	Oracle Solaris 11

Configuration Overview

Cavium LiquidSecurity HSM

The Cavium LiquidSecurity HSM used in this test is configured with reference to section 5 of the Cavium LiquidSecurity Getting Started guide LiquidSecurity-GettingStarted-Guide_r2.5_PR.pdf available for download at the Cavium Technical Support Web Site at https://support.cavium.com

Edit the `liquidsec_mgmt_util.cfg` file to use the correct "hostname", “port” and “owner_cert_path” of your HSM.



```
{
        "servers": [
        {
                "name" : "server1",
                "hostname" : "192.168.10.182",
                "port" : 48063,
                "certificate": "/home/liquidsec_bin/data/cert-c",
                "pkey": "/home/liquidsec_bin/data/pkey-c",
                "CAfile": "",
                "CApath": "/home/liquidsec_bin/data/ssl/certs",
                "ssl_ciphers": "",
                "server_ssl" : "yes",
        "enable"    : "yes",
                "e2e_encryption": {
                        "enable":"yes",
                        "owner_cert_path":"/home/liquidsec_bin/data/PO.crt"
                },
        },{
                "name" : "server2",
                "hostname" : "www.vHSM2.com",
                "port" : 3225,
                "certificate": "cert-c",
                "pkey": "pkey-c",
                "CAfile": "",
                "CApath": "/home/liquidsec_bin/data/ssl/certs",
                "ssl_ciphers": "",
                "server_ssl" : "yes",
        "enable"    : "no",
                "e2e_encryption": {
                        "enable":"yes",
                        "owner_cert_path":"PO.crt"
                },
        }],

    "scard": {
        "enable": "no",
        "port": 48063,
        "certificate": "cert-sc",
        "pkey": "pkey-sc",
    }
}
~
~
~
                                                                      5,31-45       All
```

Initialization of the Cavium LiquidSecurity HSM

Generate Partition Owner Key (POK) and certificate (TA(PO)):

```
$openssl req -newkey rsa:2048 -nodes -keyout PO.key -x509
-days 365 -out PO.crt
```

Start `liquidsec_mgmt_util` with the configuration file and initialize the partition:

```
/home/liquidsec_bin/bin/liquidsec_mgmt_util /home/liquidsec_bin/data/liquidsec_mgmt_util.cfg
```

a. Run the following command:

```
cloudmgmt> server 0
```

b. Initialize the partition.

When running `liquidsec_mgmt_util` for the first time, you must complete the following steps:

```
server0> enable_unencrypted
server0> zeroizeHSM
server0> loginHSM CO cavium default
server0> initHSM hsm_config crypto_officer so12345 1
*************************CAUTION********************************
This is a CRITICAL operation, should NOT be done when server(s)
is in a cluster.
Cav Server will exit if Node ID or appliance user details
are different in Cav Server conf file from command inputs.
Cav Server will have to be restarted after correcting conf file
****************************************************************
Do you want to continue(y/n)?y
BACKUP By MCO 1
Block delete user 1
Creating AU user.
User Name: app_user
Password: user1234567890
initHSM success
```

After running the `initHSM` command, the partition will have a preCO officer (with very limited privileges) with the user name `crypto_officer`. By default, the appliance user will also be created with username `app_user` and password `user1234567890`.

Run the following commands to proceed further:

```
server0> loginHSM PO crypto_officer so12345
```

Get partition CSR.

```
server0> getCertReq P1.csr
```

Open a new terminal window from the data directory and sign the HSM CSR with the TA(PO) cert-key pair.

```
# openssl x509 -days 365 -req -in P1.csr -CA PO.crt -CAkey PO.key -set_serial 01 -out POsigned.crt
```

Store the partition owner certificate TA(PO) and partition owner signed partition certificate Cert_PO(P).

```
server0> storeCert PO.crt 4
server0> storeCert POsigned.crt 8
```

Change password of preCO user.

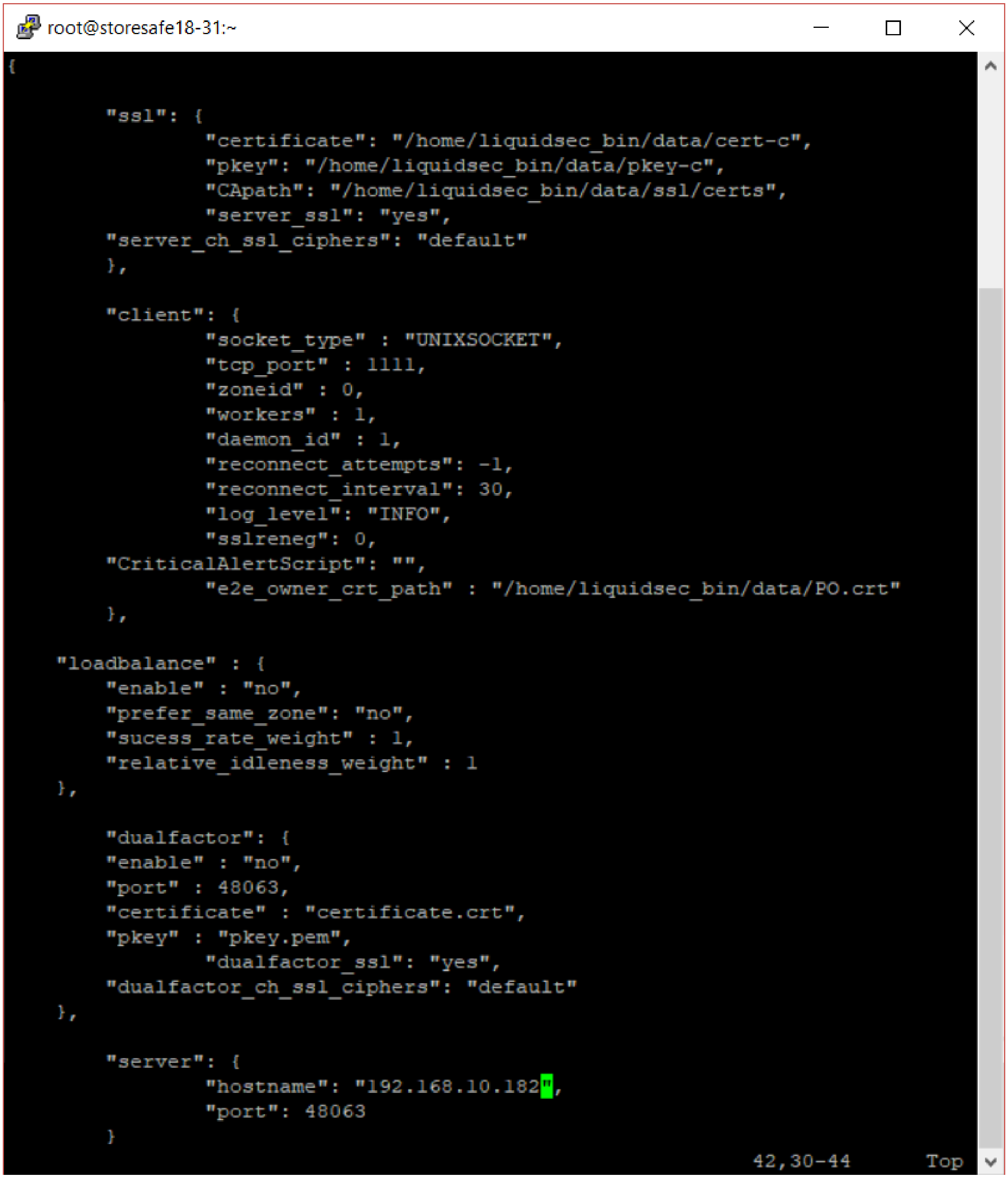
```
server0>changePswd PO crypto_officer so12345
server0>logoutHSM
server0>exit
```

At this point you can log in as the partition Crypto Officer (PCO).

```
cloudmgmt>enable_e2e
cloudmgmt>server 0
server0>loginHSM CO crypto_officer so12345
server0>createUser CU bloombase 12345678
server0>exit
cloudmgmt>quit
```

Connecting to Cavium LiquidSecurity HSM

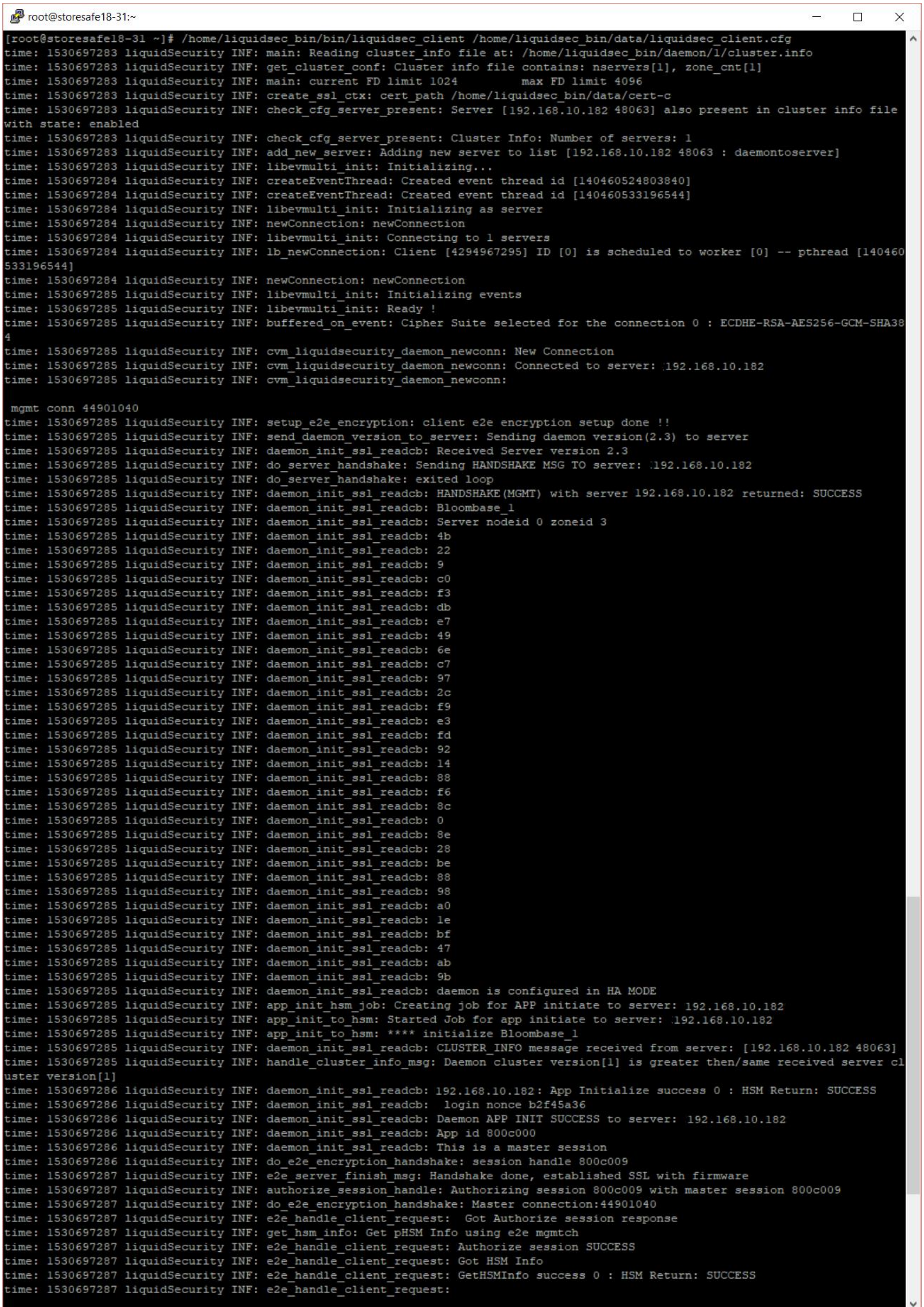
Edit the `liquidsec_client.cfg` file to use the correct "hostname", “port” and “owner_cert_path” of your HSM.



```
{

        "ssl": {
                "certificate": "/home/liquidsec_bin/data/cert-c",
                "pkey": "/home/liquidsec_bin/data/pkey-c",
                "CApath": "/home/liquidsec_bin/data/ssl/certs",
                "server_ssl": "yes",
        "server_ch_ssl_ciphers": "default"
        },

        "client": {
                "socket_type" : "UNIXSOCKET",
                "tcp_port" : 1111,
                "zoneid" : 0,
                "workers" : 1,
                "daemon_id" : 1,
                "reconnect_attempts": -1,
                "reconnect_interval": 30,
                "log_level": "INFO",
                "sslreneg": 0,
        "CriticalAlertScript": "",
                "e2e_owner_crt_path" : "/home/liquidsec_bin/data/PO.crt"
        },

    "loadbalance" : {
        "enable" : "no",
        "prefer_same_zone": "no",
        "sucess_rate_weight" : 1,
        "relative_idleness_weight" : 1
    },

        "dualfactor": {
        "enable" : "no",
        "port" : 48063,
        "certificate" : "certificate.crt",
        "pkey" : "pkey.pem",
                "dualfactor_ssl": "yes",
        "dualfactor_ch_ssl_ciphers": "default"
    },

        "server": {
                "hostname": "192.168.10.182",
                "port": 48063
        }
                                                                  42,30-44        Top
```

Run a Single Instance of the `liquidsec_client` using your configuration file

```
$/home/liquidsec_bin/bin/liquidsec_client /home/liquidsec_bin/data/liquidsec_client.cfg
```



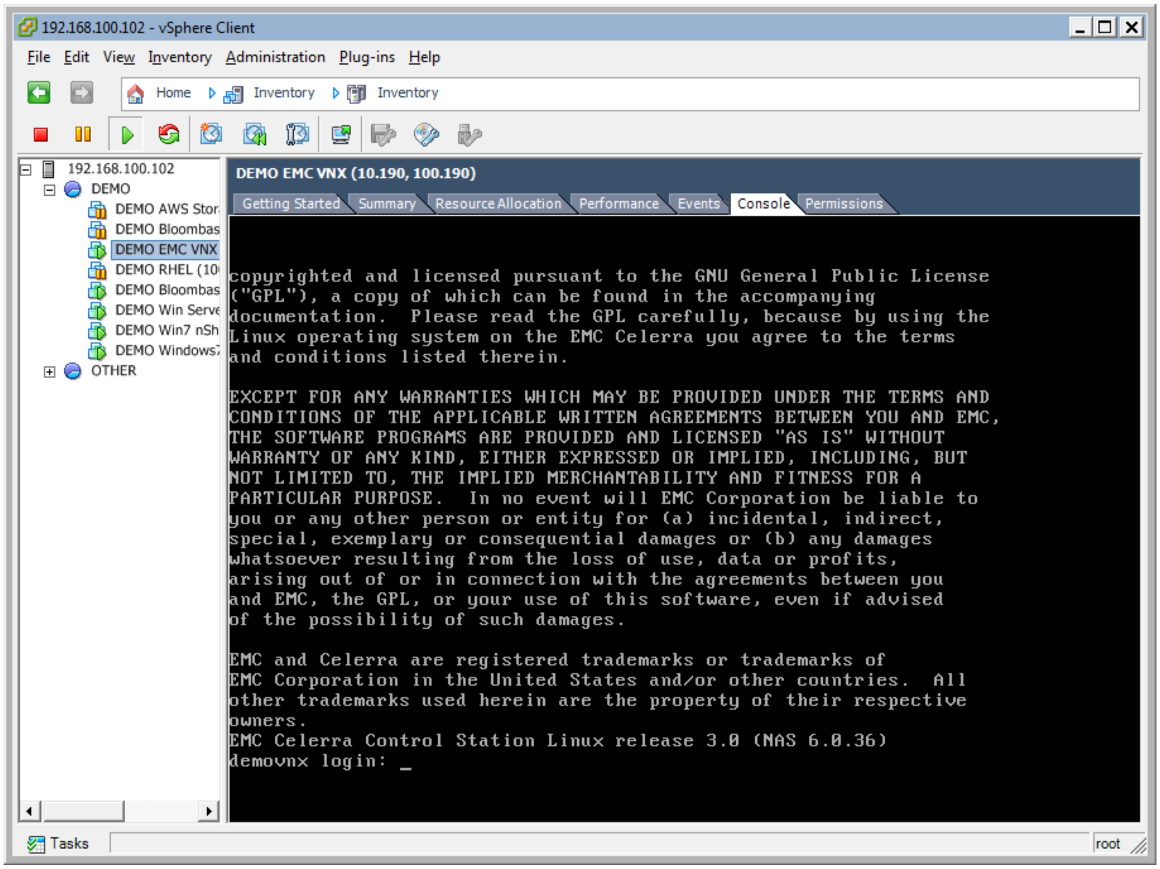
```
[root@storesafe18-31 ~]# /home/liquidsec_bin/bin/liquidsec_client /home/liquidsec_bin/data/liquidsec_client.cfg
time: 1530697283 liquidSecurity INF: main: Reading cluster_info file at: /home/liquidsec_bin/daemon/1/cluster.info
time: 1530697283 liquidSecurity INF: get_cluster_conf: Cluster info file contains: nservers[1], zone_cnt[1]
time: 1530697283 liquidSecurity INF: main: current FD limit 1024         max FD limit 4096
time: 1530697283 liquidSecurity INF: create_ssl_ctx: cert_path /home/liquidsec_bin/data/cert-c
time: 1530697283 liquidSecurity INF: check_cfg_server_present: Server [192.168.10.182 48063] also present in cluster info file
with state: enabled
time: 1530697283 liquidSecurity INF: check_cfg_server_present: Cluster Info: Number of servers: 1
time: 1530697283 liquidSecurity INF: add_new_server: Adding new server to list [192.168.10.182 48063 : daemontoserver]
time: 1530697283 liquidSecurity INF: libevmulti_init: Initializing...
time: 1530697284 liquidSecurity INF: createEventThread: Created event thread id [140460524803840]
time: 1530697284 liquidSecurity INF: createEventThread: Created event thread id [140460533196544]
time: 1530697284 liquidSecurity INF: libevmulti_init: Initializing as server
time: 1530697284 liquidSecurity INF: newConnection: newConnection
time: 1530697284 liquidSecurity INF: libevmulti_init: Connecting to 1 servers
time: 1530697284 liquidSecurity INF: lb_newConnection: Client [4294967295] ID [0] is scheduled to worker [0] -- pthread [140460
533196544]
time: 1530697284 liquidSecurity INF: newConnection: newConnection
time: 1530697285 liquidSecurity INF: libevmulti_init: Initializing events
time: 1530697285 liquidSecurity INF: libevmulti_init: Ready !
time: 1530697285 liquidSecurity INF: buffered_on_event: Cipher Suite selected for the connection 0 : ECDHE-RSA-AES256-GCM-SHA38
4
time: 1530697285 liquidSecurity INF: cvm_liquidsecurity_daemon_newconn: New Connection
time: 1530697285 liquidSecurity INF: cvm_liquidsecurity_daemon_newconn: Connected to server: 192.168.10.182
time: 1530697285 liquidSecurity INF: cvm_liquidsecurity_daemon_newconn:

 mgmt conn 44901040
time: 1530697285 liquidSecurity INF: setup_e2e_encryption: client e2e encryption setup done !!
time: 1530697285 liquidSecurity INF: send_daemon_version_to_server: Sending daemon version(2.3) to server
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: Received Server version 2.3
time: 1530697285 liquidSecurity INF: do_server_handshake: Sending HANDSHAKE MSG TO server: 192.168.10.182
time: 1530697285 liquidSecurity INF: do_server_handshake: exited loop
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: HANDSHAKE(MGMT) with server 192.168.10.182 returned: SUCCESS
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: Bloombase_1
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: Server nodeid 0 zoneid 3
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 4b
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 22
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 9
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: c0
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: f3
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: db
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: e7
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 49
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 6e
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: c7
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 97
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 2c
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: f9
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: e3
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: fd
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 92
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 14
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 88
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: f6
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 8c
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 0
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 8e
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 28
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: be
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 88
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 98
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: a0
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 1e
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: bf
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 47
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: ab
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: 9b
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: daemon is configured in HA MODE
time: 1530697285 liquidSecurity INF: app_init_hsm_job: Creating job for APP initiate to server: 192.168.10.182
time: 1530697285 liquidSecurity INF: app_init_to_hsm: Started Job for app initiate to server: 192.168.10.182
time: 1530697285 liquidSecurity INF: app_init_to_hsm: **** initialize Bloombase_1
time: 1530697285 liquidSecurity INF: daemon_init_ssl_readcb: CLUSTER_INFO message received from server: [192.168.10.182 48063]
time: 1530697285 liquidSecurity INF: handle_cluster_info_msg: Daemon cluster version[1] is greater then/same received server cl
uster version[1]
time: 1530697286 liquidSecurity INF: daemon_init_ssl_readcb: 192.168.10.182: App Initialize success 0 : HSM Return: SUCCESS
time: 1530697286 liquidSecurity INF: daemon_init_ssl_readcb:  login nonce b2f45a36
time: 1530697286 liquidSecurity INF: daemon_init_ssl_readcb: Daemon APP INIT SUCCESS to server: 192.168.10.182
time: 1530697286 liquidSecurity INF: daemon_init_ssl_readcb: App id 800c000
time: 1530697286 liquidSecurity INF: daemon_init_ssl_readcb: This is a master session
time: 1530697286 liquidSecurity INF: do_e2e_encryption_handshake: session handle 800c009
time: 1530697287 liquidSecurity INF: e2e_server_finish_msg: Handshake done, established SSL with firmware
time: 1530697287 liquidSecurity INF: authorize_session_handle: Authorizing session 800c009 with master session 800c009
time: 1530697287 liquidSecurity INF: do_e2e_encryption_handshake: Master connection:44901040
time: 1530697287 liquidSecurity INF: e2e_handle_client_request:  Got Authorize session response
time: 1530697287 liquidSecurity INF: get_hsm_info: Get pHSM Info using e2e mgmtch
time: 1530697287 liquidSecurity INF: e2e_handle_client_request: Authorize session SUCCESS
time: 1530697287 liquidSecurity INF: e2e_handle_client_request: Got HSM Info
time: 1530697287 liquidSecurity INF: e2e_handle_client_request: GetHSMInfo success 0 : HSM Return: SUCCESS
time: 1530697287 liquidSecurity INF: e2e_handle_client_request:
```

Restart the StoreSafe service to effect the changes

```
$systemctl restart storesafe
```

Dell EMC VNX Storage System

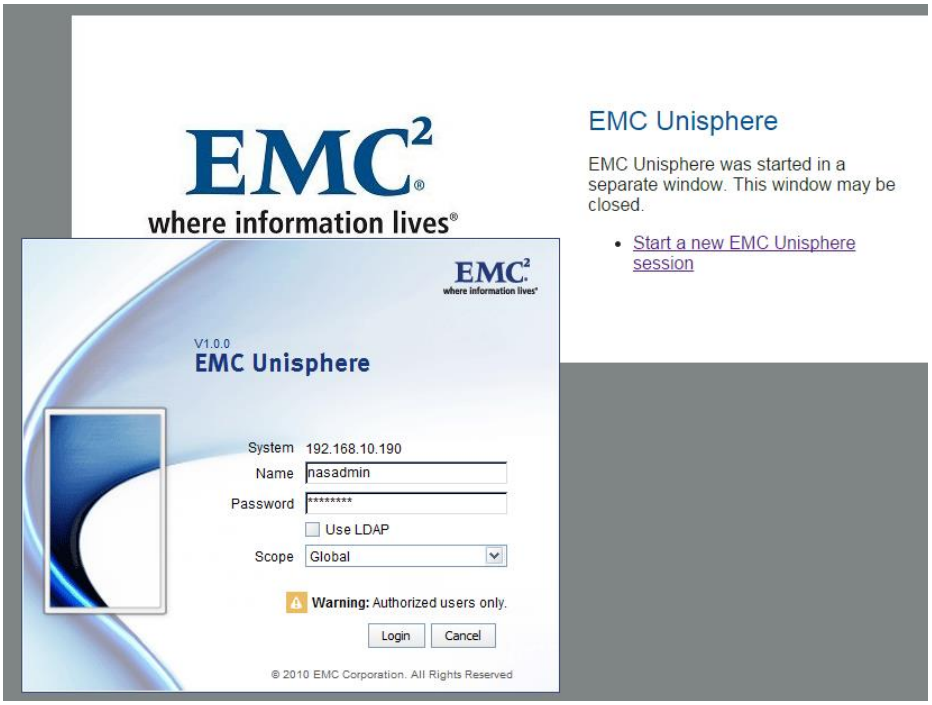
Dell EMC VNX virtual appliance is used in this interoperability test which is able to provide storage services over network storage protocols including NFS, CIFS, SMB, iSCSI, etc.



192.168.100.102 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
192.168.100.102
DEMO
DEMO AWS Stor
DEMO Bloombas
DEMO EMC VNX
DEMO RHEL (10
DEMO Bloombas
DEMO Win Serve
DEMO Win7 nSh
DEMO Windows
OTHER
DEMO EMC VNX (10.190, 100.190)
Getting Started Summary Resource Allocation Performance Events Console Permissions
Tasks
root

```
copyrighted and licensed pursuant to the GNU General Public License
("GPL"), a copy of which can be found in the accompanying
documentation.  Please read the GPL carefully, because by using the
Linux operating system on the EMC Celerra you agree to the terms
and conditions listed therein.

EXCEPT FOR ANY WARRANTIES WHICH MAY BE PROVIDED UNDER THE TERMS AND
CONDITIONS OF THE APPLICABLE WRITTEN AGREEMENTS BETWEEN YOU AND EMC,
THE SOFTWARE PROGRAMS ARE PROVIDED AND LICENSED "AS IS" WITHOUT
WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT
NOT LIMITED TO, THE IMPLIED MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE.  In no event will EMC Corporation be liable to
you or any other person or entity for (a) incidental, indirect,
special, exemplary or consequential damages or (b) any damages
whatsoever resulting from the loss of use, data or profits,
arising out of or in connection with the agreements between you
and EMC, the GPL, or your use of this software, even if advised
of the possibility of such damages.

EMC and Celerra are registered trademarks or trademarks of
EMC Corporation in the United States and/or other countries.  All
other trademarks used herein are the property of their respective
owners.
EMC Celerra Control Station Linux release 3.0 (NAS 6.0.36)
demovnx login: _
```

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



EMC Unisphere

EMC Unisphere was started in a separate window. This window may be closed.

- Start a new EMC Unisphere session

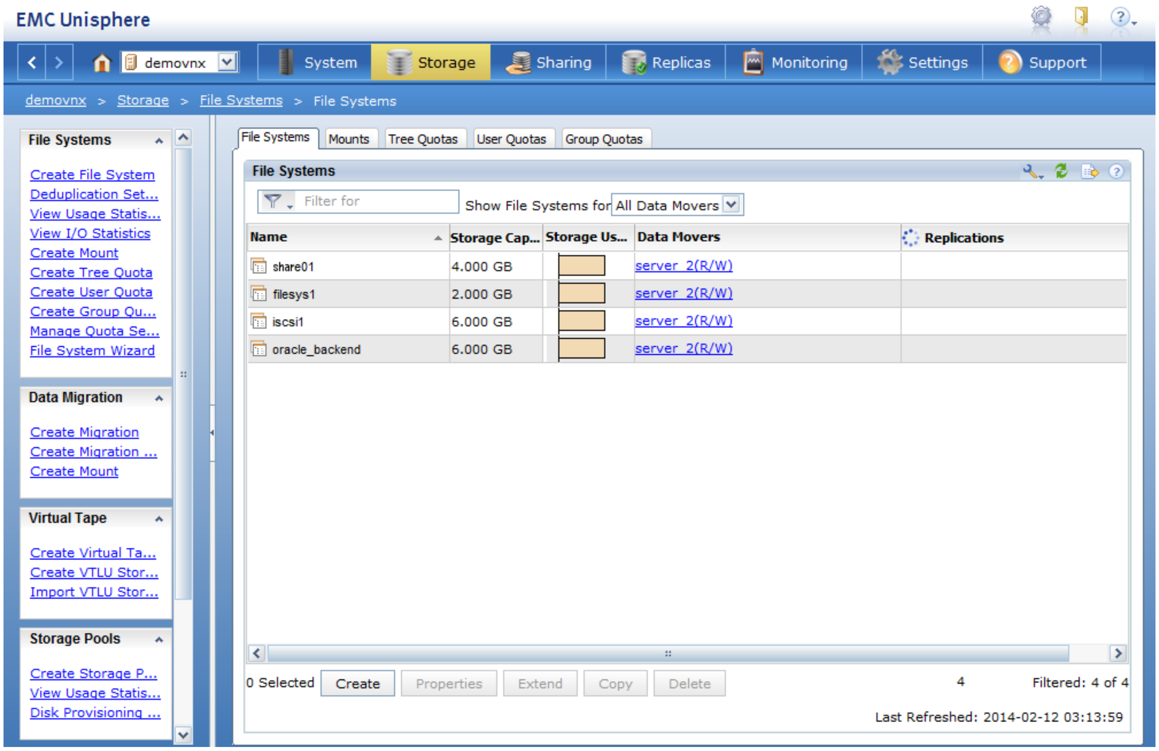
V1.0.0
EMC Unisphere

System	192.168.10.190
Name	nasadmin
Password	********
	□ Use LDAP
Scope	Global

Warning: Authorized users only.

EMC2 where information lives
Login
Cancel
© 2010 EMC Corporation. All Rights Reserved

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



EMC Unisphere

demovnx > Storage > File Systems > File Systems

File Systems

Show File Systems for All Data Movers

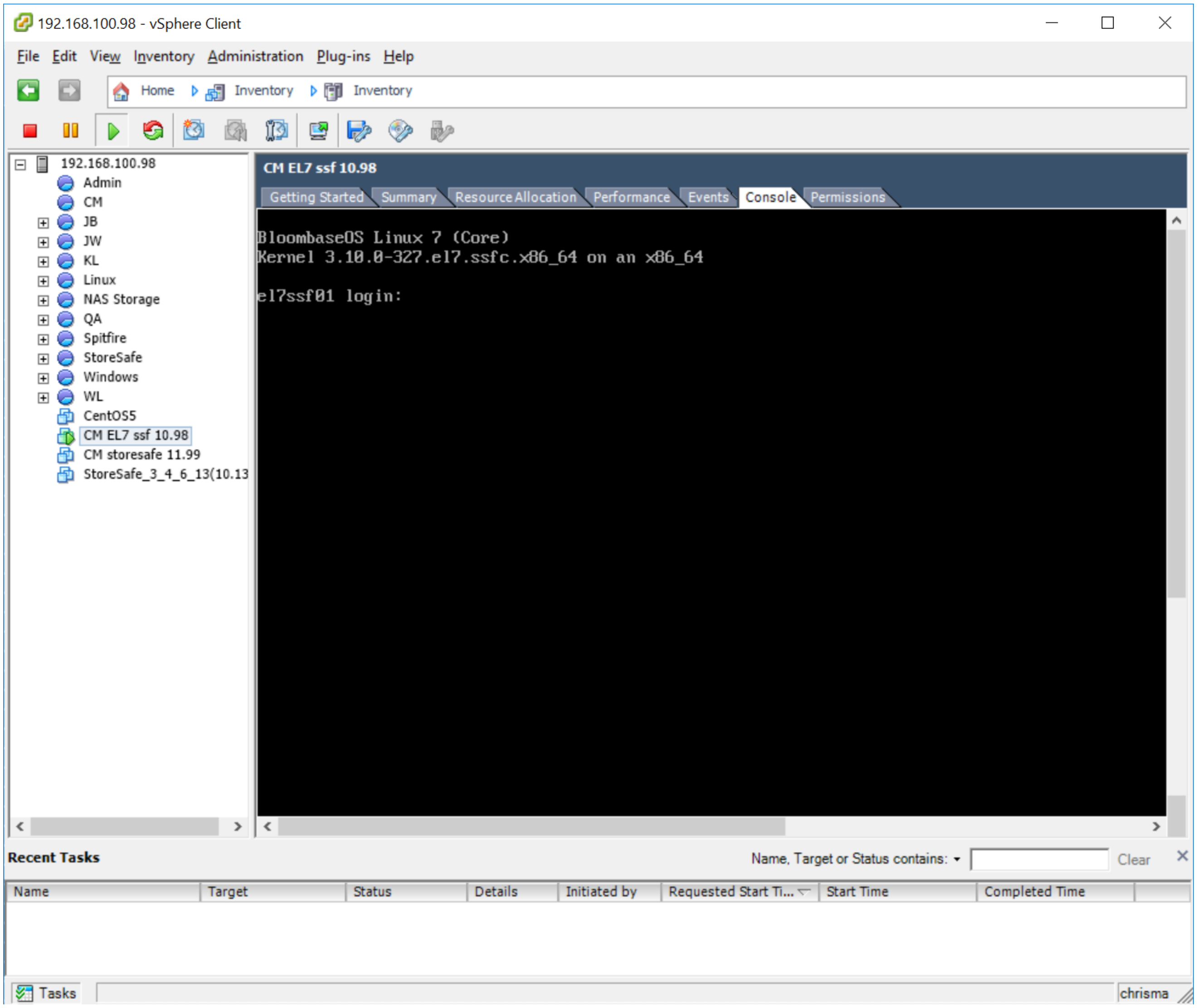
Name	Storage Cap...	Storage Us...	Data Movers	Replications
share01	4.000 GB		server_2(R/W)	
filesys1	2.000 GB		server_2(R/W)	
iscsi1	6.000 GB		server_2(R/W)	
oracle_backend	6.000 GB		server_2(R/W)	

0 Selected 4 Filtered: 4 of 4

Last Refreshed: 2014-02-12 03:13:59

Bloombase StoreSafe

Bloombase StoreSafe delivers unified data-at-rest encryption security of block devices, network shares, file services, object stores, sequential storage devices, and cloud storage services, etc. In this interoperability test, file-based encryption security services are validated against Bloombase StoreSafe with keys managed at Cavium LiquidSecurity HSM.


192.168.100.98 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
192.168.100.98
Admin
CM
JB
JW
KL
Linux
NAS Storage
QA
Spitfire
StoreSafe
Windows
WL
CentOS5
CM EL7 ssf 10.98
CM storesafe 11.99
StoreSafe_3_4_6_13(10.13
CM 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:
```

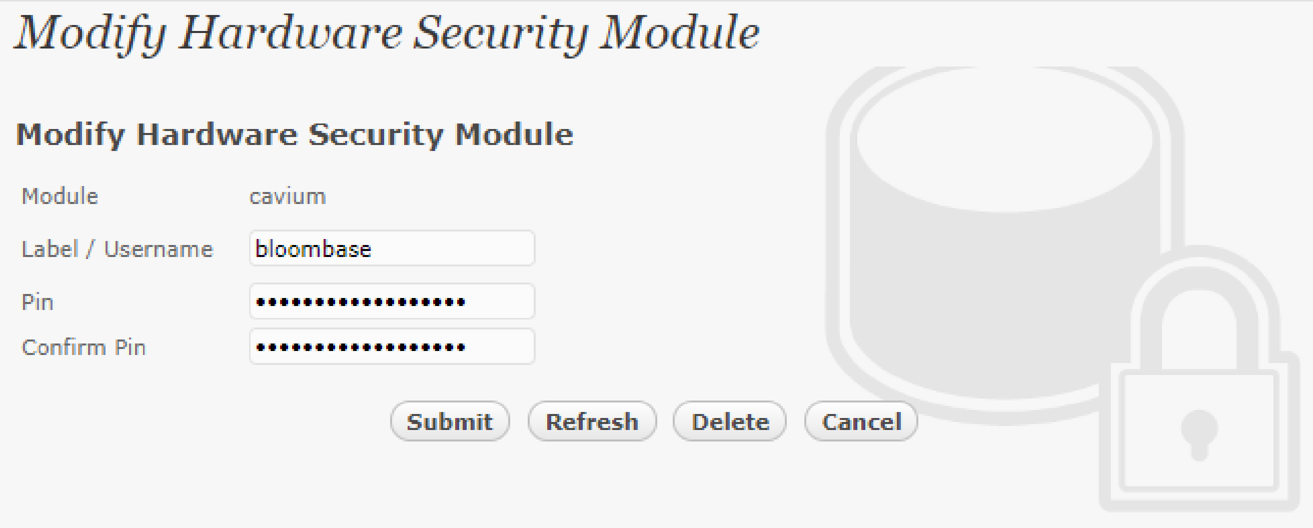
Bloombase StoreSafe software appliance is deployed as a virtual appliance (VA) on VMware vSphere 6.5.

Network Security, Trust and Authentication Configuration

In this interoperability test, Bloombase StoreSafe serves as the client of Cavium LiquidSecurity HSM for encryption key access to deliver data at-rest encryption services. Authentication of Bloombase StoreSafe to the Cavium LiquidSecurity HSM is established through the specification of passphrase as covered in former section of this document.

Cavium LiquidSecurity HSM and Bloombase KeyCastle Integration

To configure Cavium LiquidSecurity HSM at Bloombase web management console, select Module as `cavium` which allows the embedded Bloombase KeyCastle module to utilize Cavium LiquidSecurity HSM driver to access Cavium LiquidSecurity HSM server over Java Cryptography Extension (JCE) provider interface.

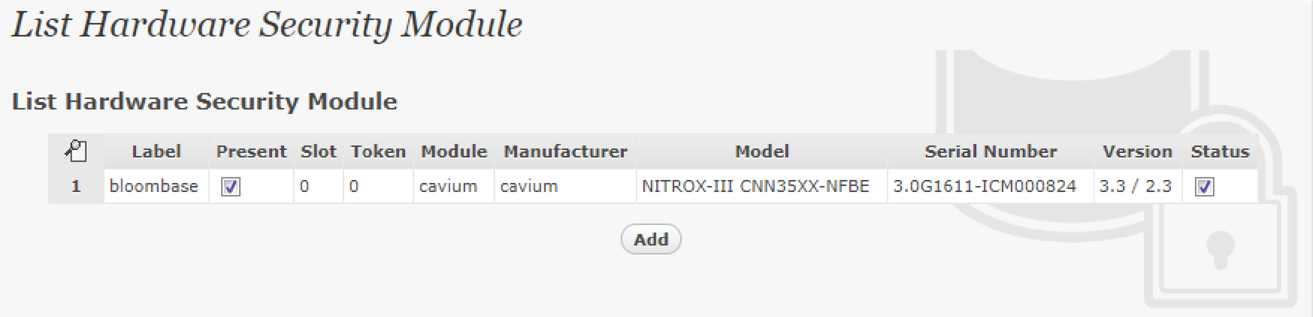


Modify Hardware Security Module

Modify Hardware Security Module

Module	cavium
Label / Username	bloombase
Pin	••••••••••••••••••
Confirm Pin	••••••••••••••••••

In this scenario, use the Cavium LiquidSecurity HSM with a crypto user `bloombase` and user pin as `Pin`. When Cavium LiquidSecurity HSM resource is properly provisioned at Bloombase StoreSafe, the `Present` and `Status` box would be checked.



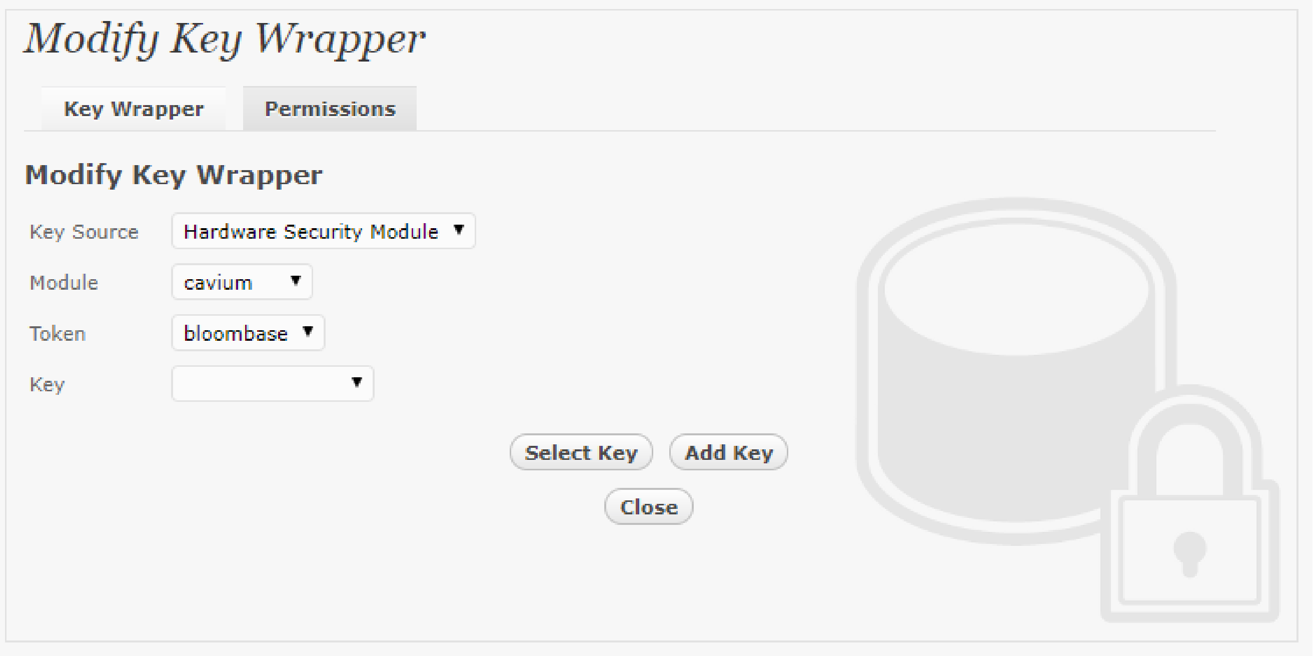
List Hardware Security Module

List Hardware Security Module

	Label	Present	Slot	Token	Module	Manufacturer	Model	Serial Number	Version	Status
1	bloombase	☑	0	0	cavium	cavium	NITROX-III CNN35XX-NFBE	3.0G1611-ICM000824	3.3 / 2.3	☑

Encryption Key Provisioning

Select Key Source as `Hardware Security Module` with Module `cavium`, assign HSM token label as `bloombase` and click `Add Key`.



Modify Key Wrapper

Modify Key Wrapper

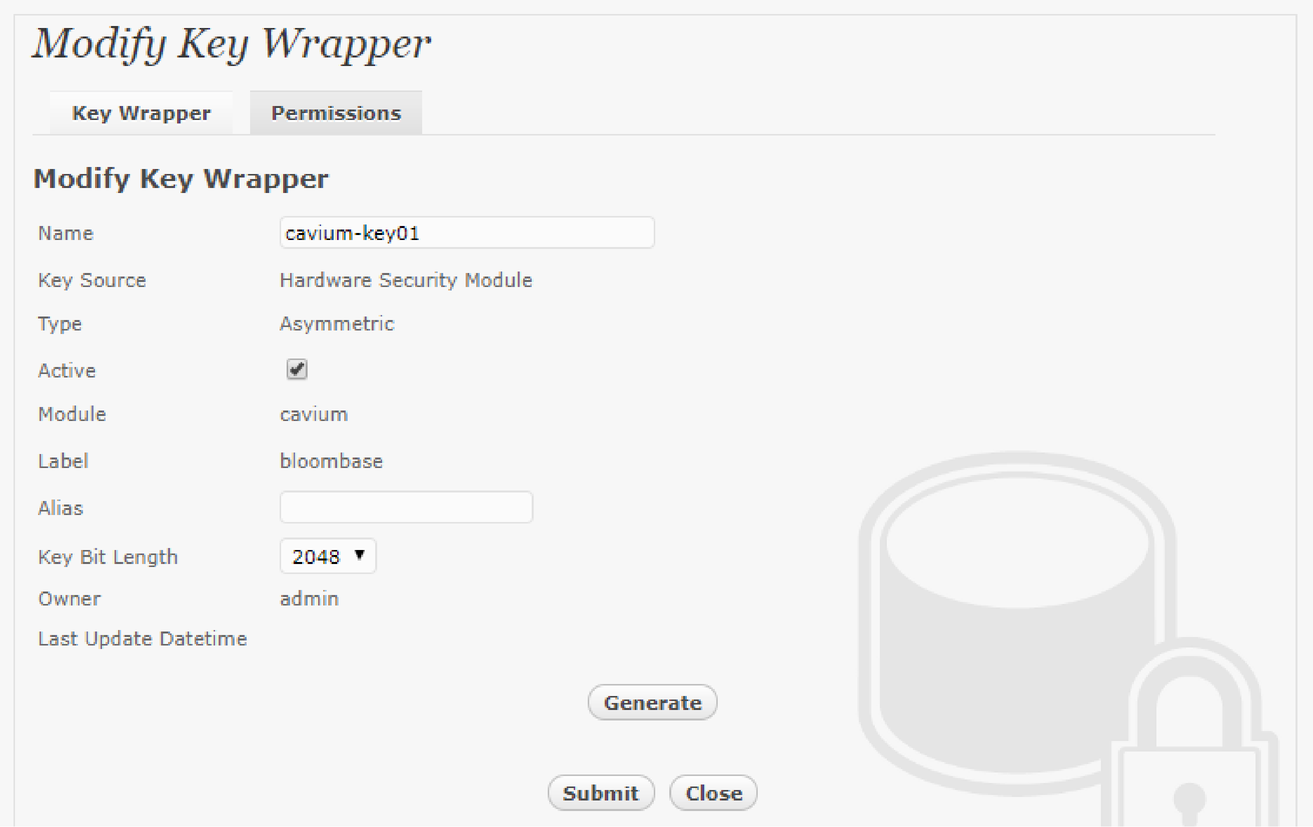
Key Source: Hardware Security Module

Module: cavium

Token: bloombase

Key:

Associate the Cavium LiquidSecurity HSM encryption key with name `cavium-key01` in bundled Bloombase KeyCastle key life-cycle management tool.

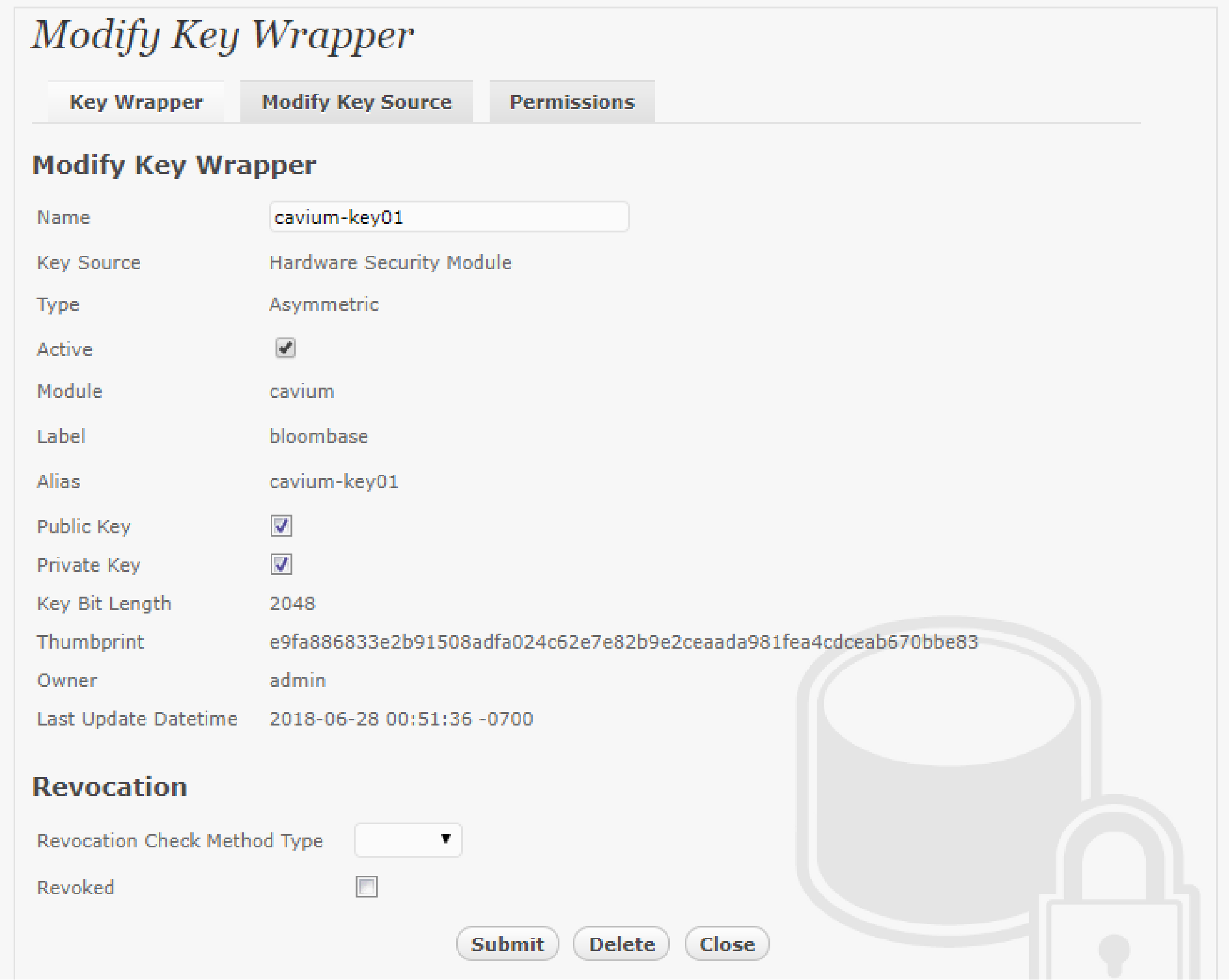


Modify Key Wrapper

Modify Key Wrapper

Name	cavium-key01
Key Source	Hardware Security Module
Type	Asymmetric
Active	☑
Module	cavium
Label	bloombase
Alias	
Key Bit Length	2048 ▼
Owner	admin
Last Update Datetime	

Click `Generate` to create the encryption key stored in Cavium LiquidSecurity HSM.



Modify Key Wrapper

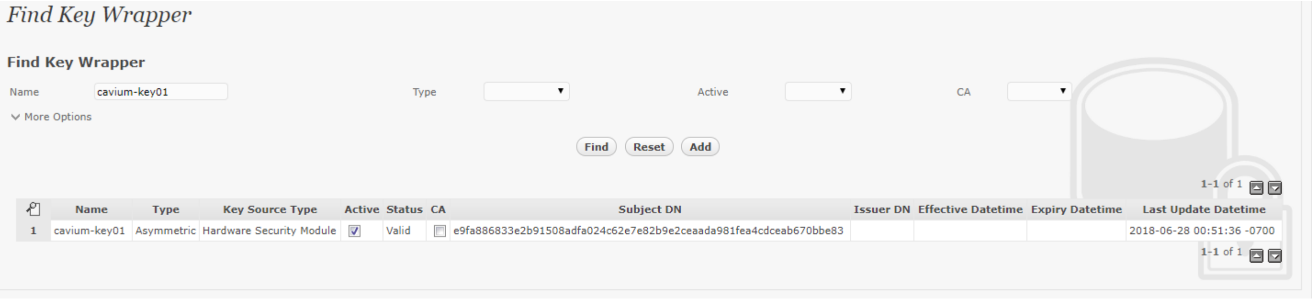
Modify Key Wrapper

Name	cavium-key01
Key Source	Hardware Security Module
Type	Asymmetric
Active	☑
Module	cavium
Label	bloombase
Alias	cavium-key01
Public Key	☑
Private Key	☑
Key Bit Length	2048
Thumbprint	e9fa886833e2b91508adfa024c62e7e82b9e2ceaada981fea4cdceab670bbe83
Owner	admin
Last Update Datetime	2018-06-28 00:51:36 -0700

Revocation

Revocation Check Method Type	▾
Revoked	□

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



Find Key Wrapper

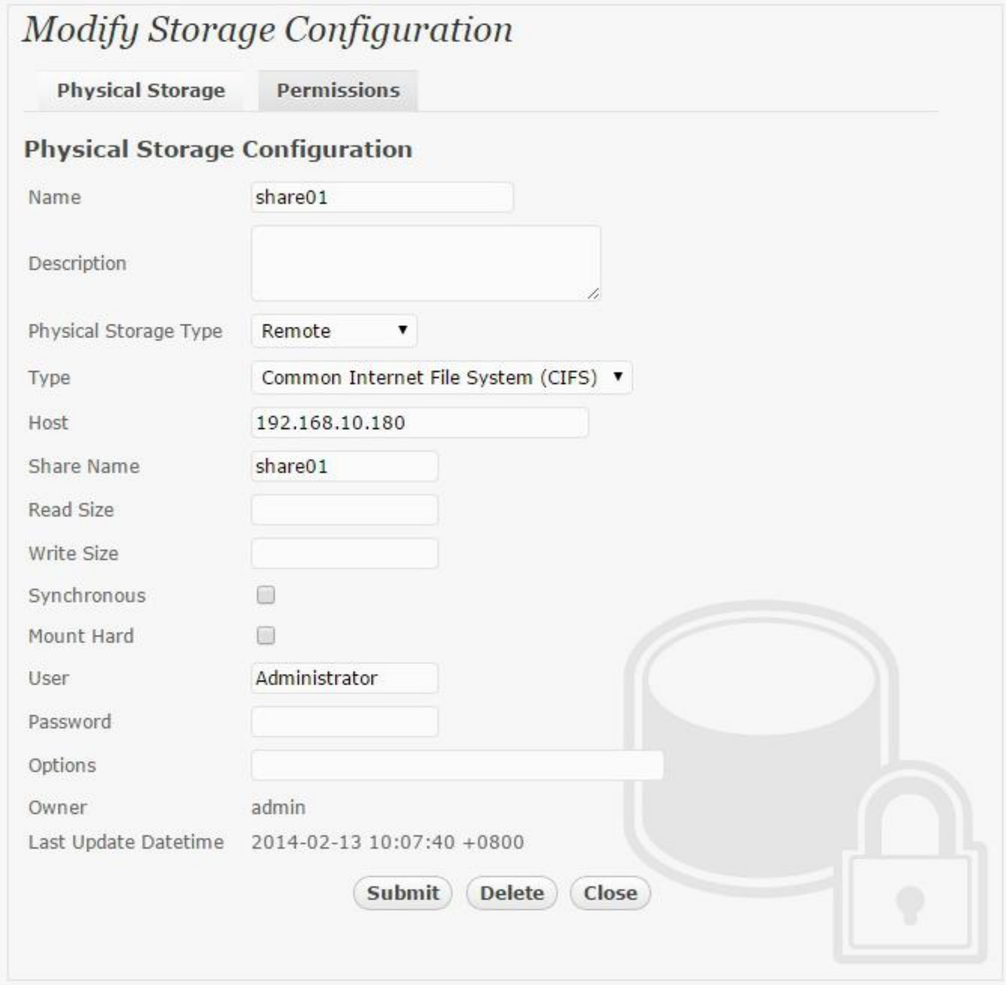
Find Key Wrapper

Name	cavium-key01	Type	▾	Active	▾	CA	▾

	Name	Type	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1	cavium-key01	Asymmetric	Hardware Security Module	☑	Valid	□	e9fa886833e2b91508adfa024c62e7e82b9e2ceaada981fea4cdceab670bbe83				2018-06-28 00:51:36 -0700

Backend Storage Configuration

Backend storage namely `share01` is configured to be secured by Bloombase StoreSafe with encryption key managed at Cavium LiquidSecurity HSM.

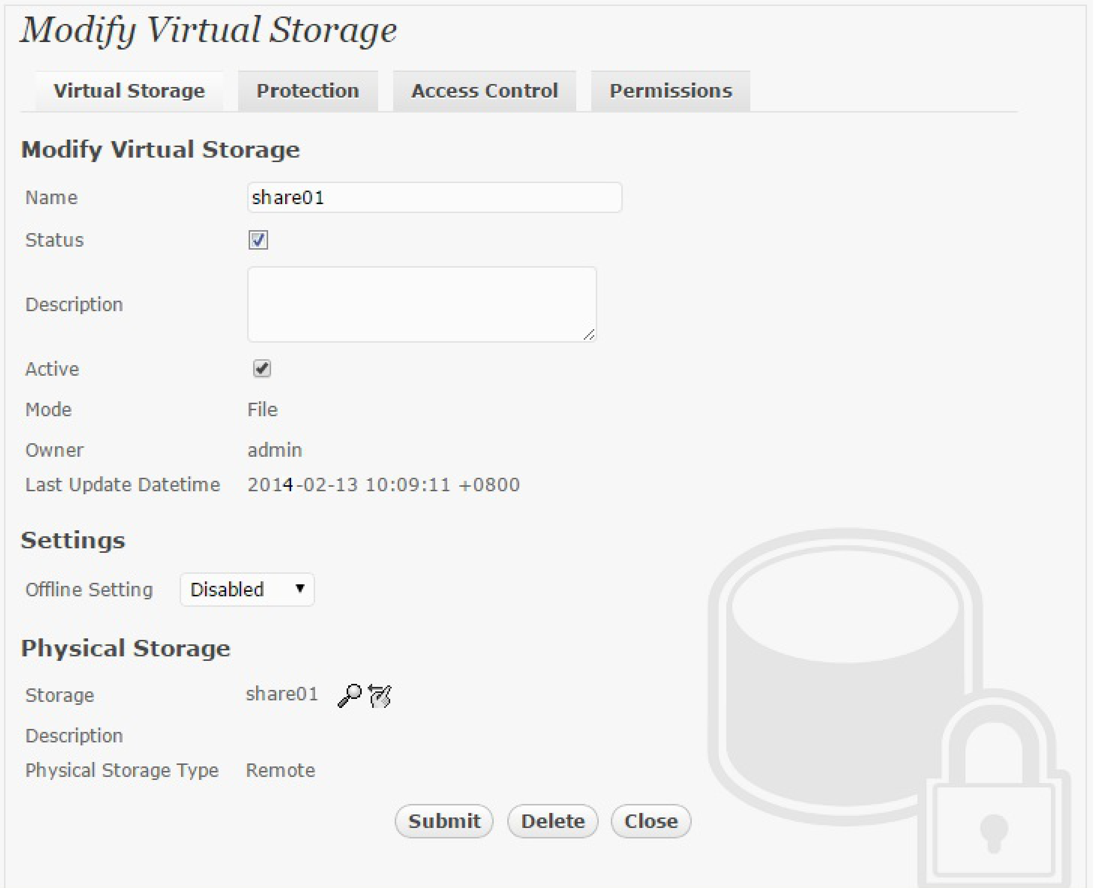


Physical Storage Configuration

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 backend storage `share01` for encryption protection over network file protocols SMB, 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

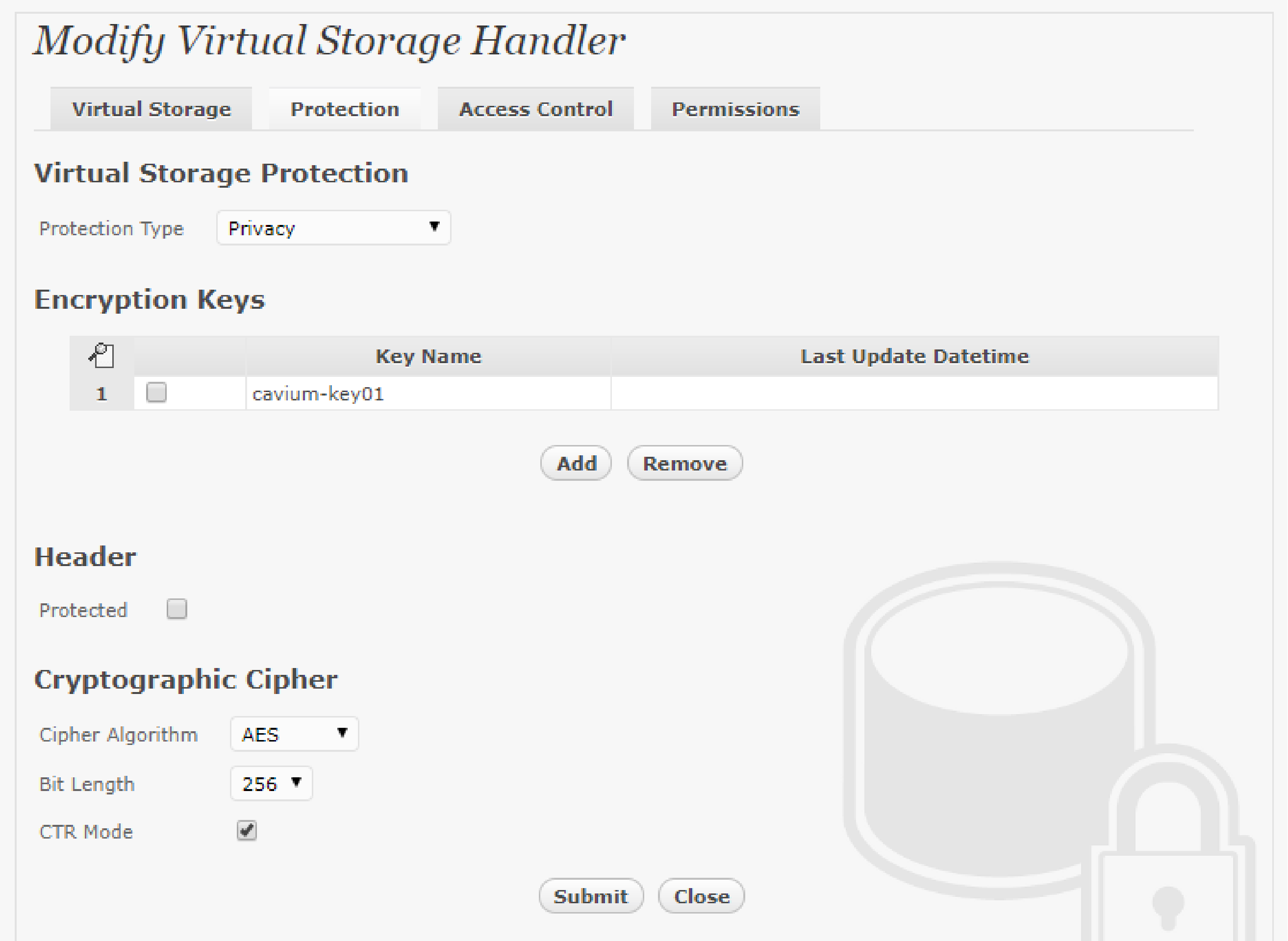
Settings

Offline Setting	Disabled

Physical Storage

Storage	share01
Description	
Physical Storage Type	Remote

Protection type is specified as `Privacy` to secure the backend Dell EMC VNX storage using `AES 256`-bit encryption by cryptographic key `cavium-key01` managed at Cavium LiquidSecurity HSM.



Modify Virtual Storage Handler

Virtual Storage Protection

Protection Type: Privacy

Encryption Keys

		Key Name	Last Update Datetime
1	□	cavium-key01	

Header

Protected □

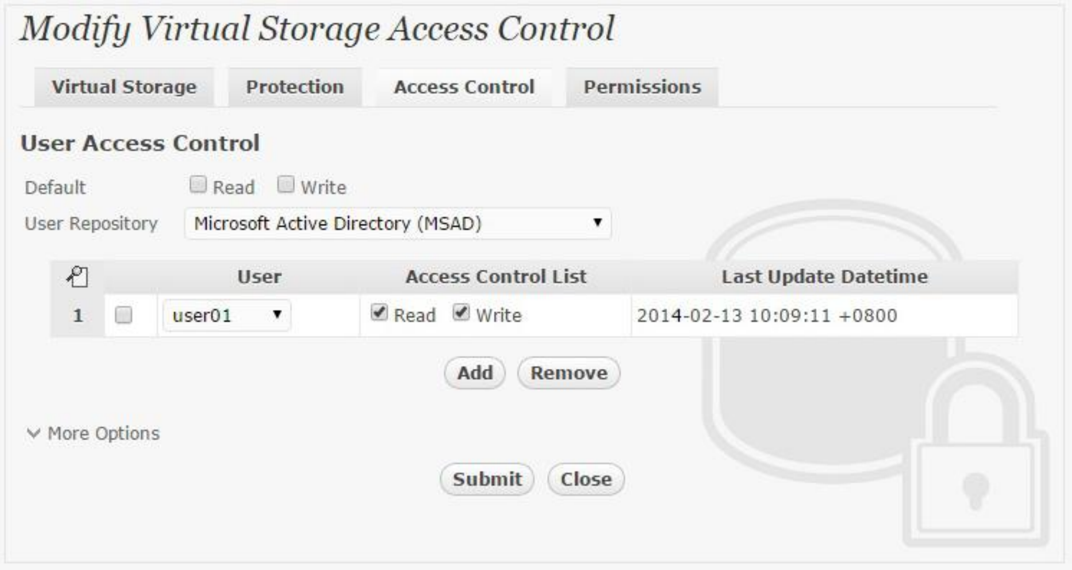
Cryptographic Cipher

Cipher Algorithm: AES

Bit Length: 256

CTR Mode ☑

SMB and CIFS storage protocols rely 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 (MSAD)` integration for user-password authentication and single sign-on.



User Access Control

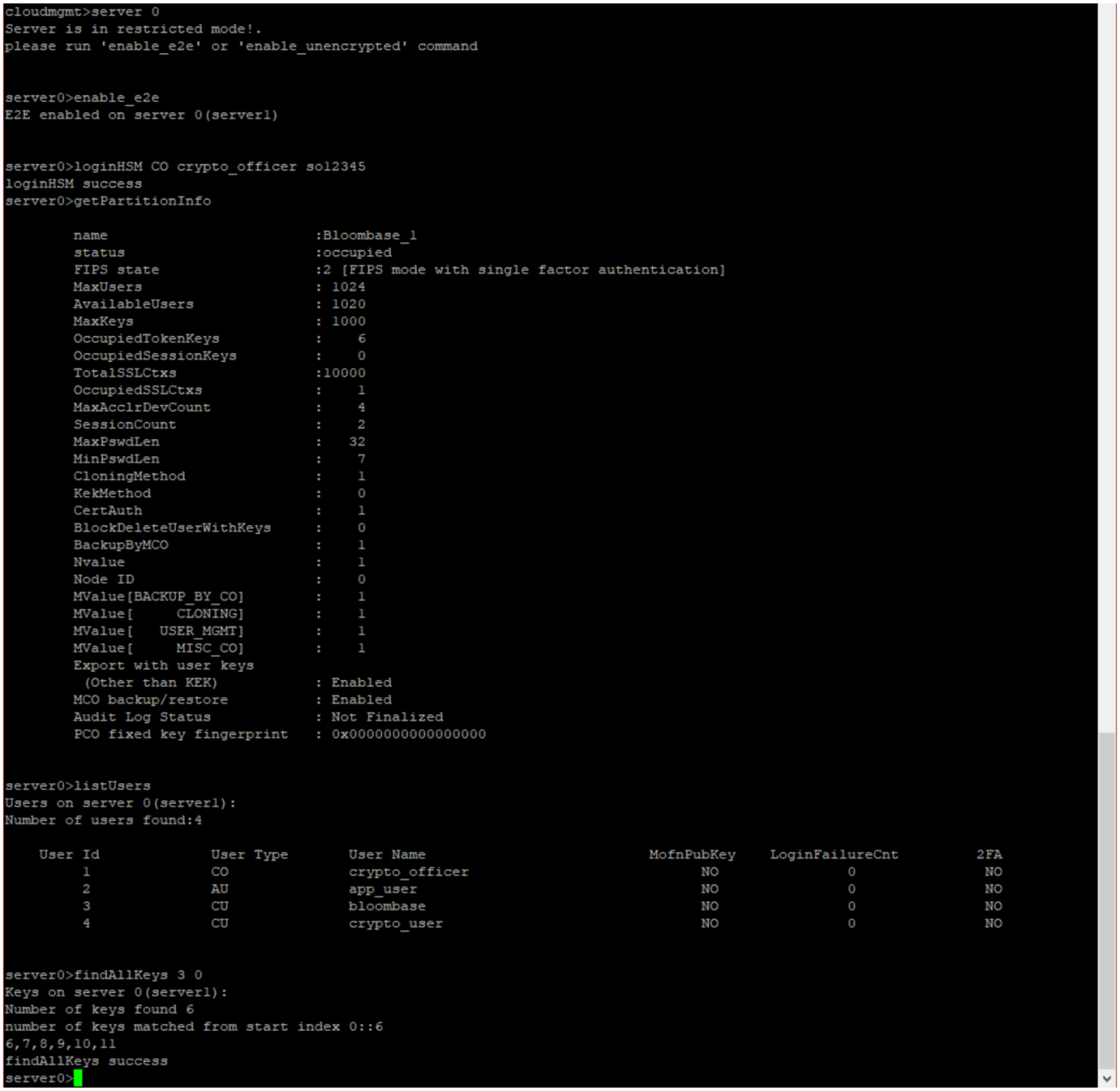
Default □ Read □ Write

User Repository: Microsoft Active Directory (MSAD)

		User	Access Control List	Last Update Datetime
1	□	user01	☑ Read ☑ Write	2014-02-13 10:09:11 +0800

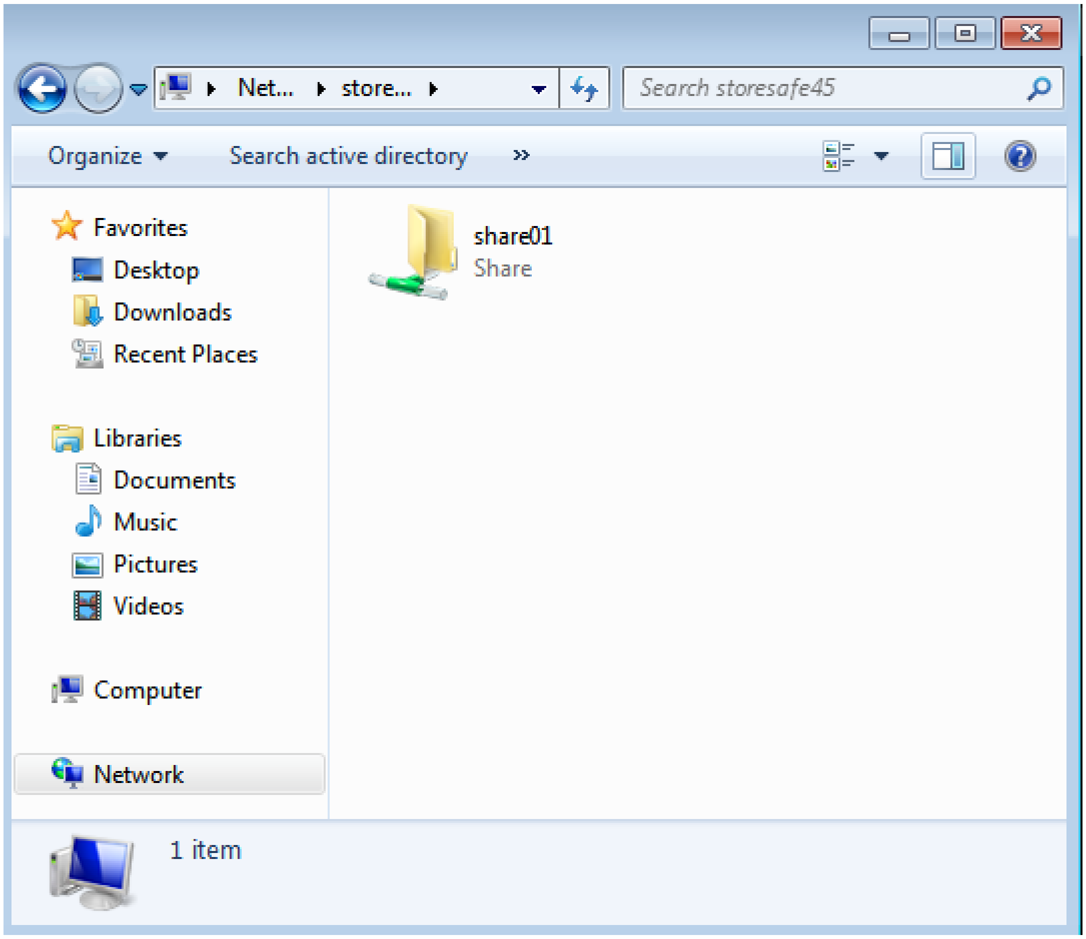
Testing

Check keys generated by HSM using `liquidsec_mgmt_util`

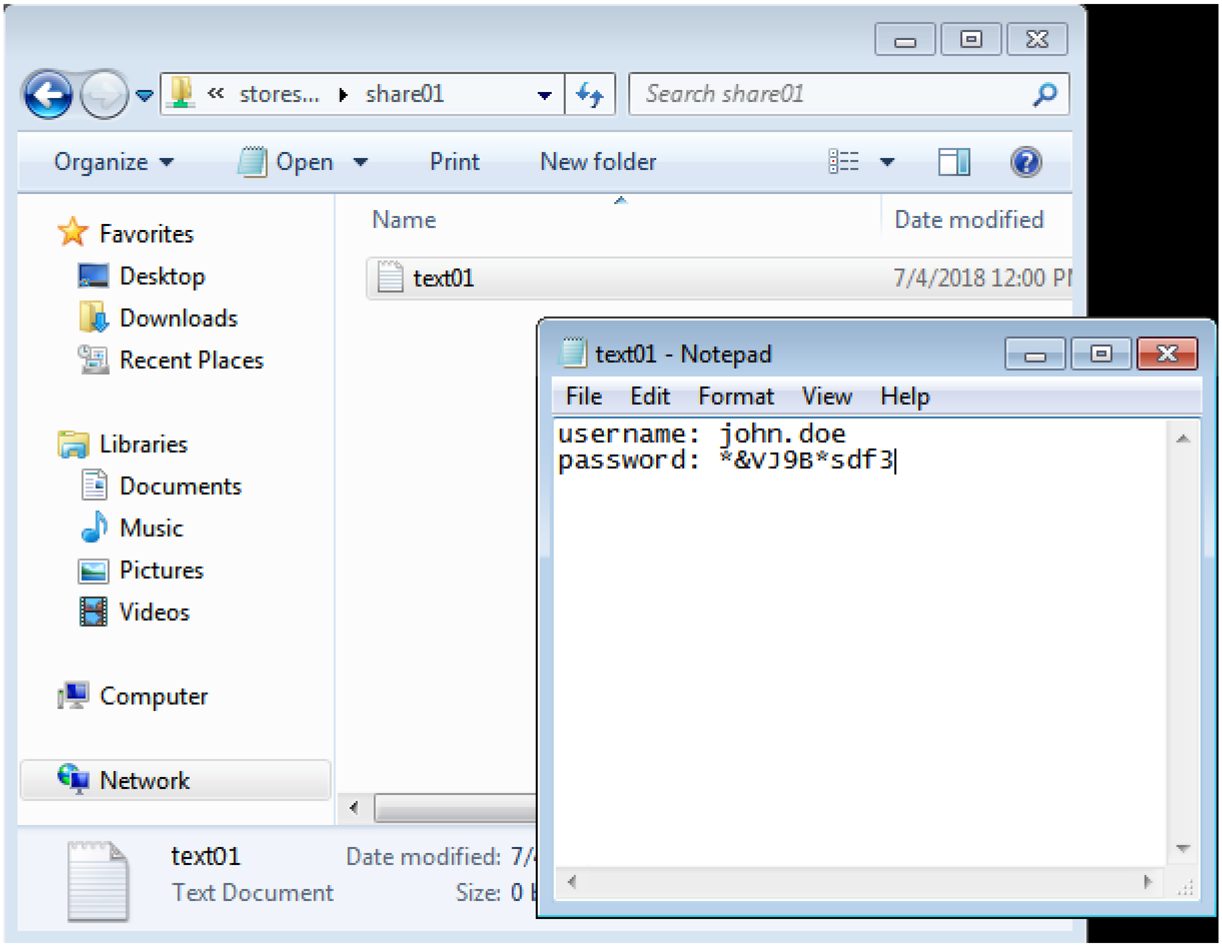


```
cloudmgmt>server 0
Server is in restricted mode!.
please run 'enable_e2e' or 'enable_unencrypted' command


server0>enable_e2e
E2E enabled on server 0(server1)


server0>loginHSM CO crypto_officer sol2345
loginHSM success
server0>getPartitionInfo

        name                        :Bloombase_1
        status                      :occupied
        FIPS state                  :2 [FIPS mode with single factor authentication]
        MaxUsers                    : 1024
        AvailableUsers              : 1020
        MaxKeys                     : 1000
        OccupiedTokenKeys           :    6
        OccupiedSessionKeys         :    0
        TotalSSLCtxs                :10000
        OccupiedSSLCtxs             :    1
        MaxAcclrDevCount            :    4
        SessionCount                :    2
        MaxPswdLen                  :   32
        MinPswdLen                  :    7
        CloningMethod               :    1
        KekMethod                   :    0
        CertAuth                    :    1
        BlockDeleteUserWithKeys     :    0
        BackupByMCO                 :    1
        Nvalue                      :    1
        Node ID                     :    0
        MValue[BACKUP_BY_CO]        :    1
        MValue[     CLONING]        :    1
        MValue[   USER_MGMT]        :    1
        MValue[     MISC_CO]        :    1
        Export with user keys
         (Other than KEK)           : Enabled
        MCO backup/restore          : Enabled
        Audit Log Status            : Not Finalized
        PCO fixed key fingerprint   : 0x0000000000000000


server0>listUsers
Users on server 0(server1):
Number of users found:4

    User Id             User Type       User Name                           MofnPubKey    LoginFailureCnt         2FA
         1              CO              crypto_officer                           NO               0               NO
         2              AU              app_user                                 NO               0               NO
         3              CU              bloombase                                NO               0               NO
         4              CU              crypto_user                              NO               0               NO


server0>findAllKeys 3 0
Keys on server 0(server1):
Number of keys found 6
number of keys matched from start index 0::6
6,7,8,9,10,11
findAllKeys success
server0>
```

Accessing Bloombase StoreSafe virtual storage from client side.

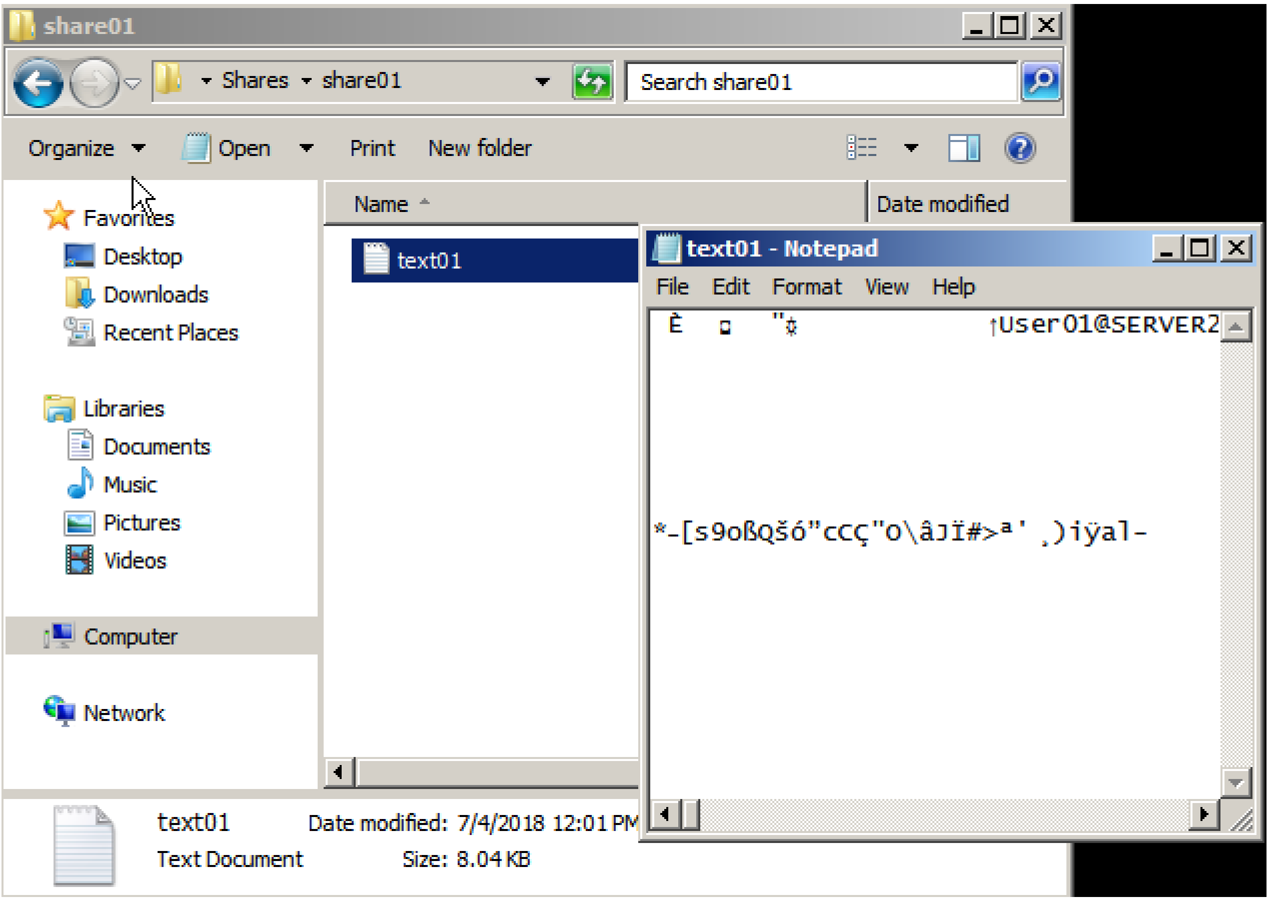


Writing a text file into StoreSafe virtual storage from client side.



```
username: john.doe
password: *&VJ9B*sdf3
```

Accessing the created file directly from backend storage will only show encrypted file content.



```
 È   ◘   "☼               ↑User01@SERVER2



*-[s9oßQšó"cCÇ"O\âJÏ#>ª' ,)iÿal-
```

text01 Date modified: 7/4/2018 12:01 PM
Text Document Size: 8.04 KB

Conclusion

Hardware Security Module

- Cavium LiquidSecurity HSM

passed all Bloombase interopLab's interoperability tests with Bloombase StoreSafe

Bloombase Product	Operating System	Hardware Security Module
Bloombase StoreSafe	Microsoft Windows Server	Cavium LiquidSecurity HSM
	Red Hat Enterprise Linux (RHEL)	Cavium LiquidSecurity HSM
	SUSE Linux Enterprise Server (SLES)	Cavium LiquidSecurity HSM
	Oracle Solaris	Cavium LiquidSecurity HSM
	IBM AIX	Cavium LiquidSecurity HSM
	HP-UX	Cavium LiquidSecurity HSM

Bloombase Product	Hardware Security Module
Bloombase StoreSafe	• Cavium LiquidSecurity HSM

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 Cavium for supporting this interoperability testing, in particular, the following individuals:

- Tejinder Singh
- Anup Marwaha
- Shasi Pulijala

Technical 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. Cavium LiquidSecurity HSM, https://www.cavium.com/product-liquidsecurity.html

4. Cavium LiquidSecurity Getting Started Guide, https://support.cavium.com

5. Dell EMC VNX, https://www.dellemc.com/en-us/storage/vnx.htm

6. VMware vSphere, https://www.vmware.com/products/vsphere.html