# **interopLab**

# Interoperability of Bloombase StoreSafe and Thales Vormetric Data Security Manager (DSM) for On-premises Traditional Data Center and Off-premises Cloud Dataat-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.

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.

© 2018 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-Thales-Vormetric-Data-Security-Manager-DSM-Interoperability-USLET-EN-Ro.93

# **Table of Contents**

Table of Contents	3
Purpose and Scope	5
Assumptions	6
Infrastructure	7
Setup	7
Key Management System	9
On-premises Data-at-Rest Encryption	9
Off-premises Data-at-Rest Encryption	9
On-premises Storage	9
Off-premises Storage	10
Client Hosts	10
Configuration Overview	11
Thales Vormetric Data Security Manager (DSM)	11
Thales Vormetric Data Security Manager (DSM) Configurations	12
HPE P2000 G3 MSA Disk Array Storage System	15
Microsoft Windows Stroage Server on Microsoft Windows Server 2019	16
Amazon EFS Cloud Storage Services	18
Bloombase StoreSafe	18
Network Security, Trust and Authentication Configuration	20
Thales Vormetric Data Security Manager (DSM) and Bloombase KeyCastle Integration	20
Encryption Key Provisioning	23
Backend Physical Storage Configuration	26
Secure Storage Configuration	30
Conclusion	36
Disclaimer	38
Acknowledgement	39
Technical Reference	40

# 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

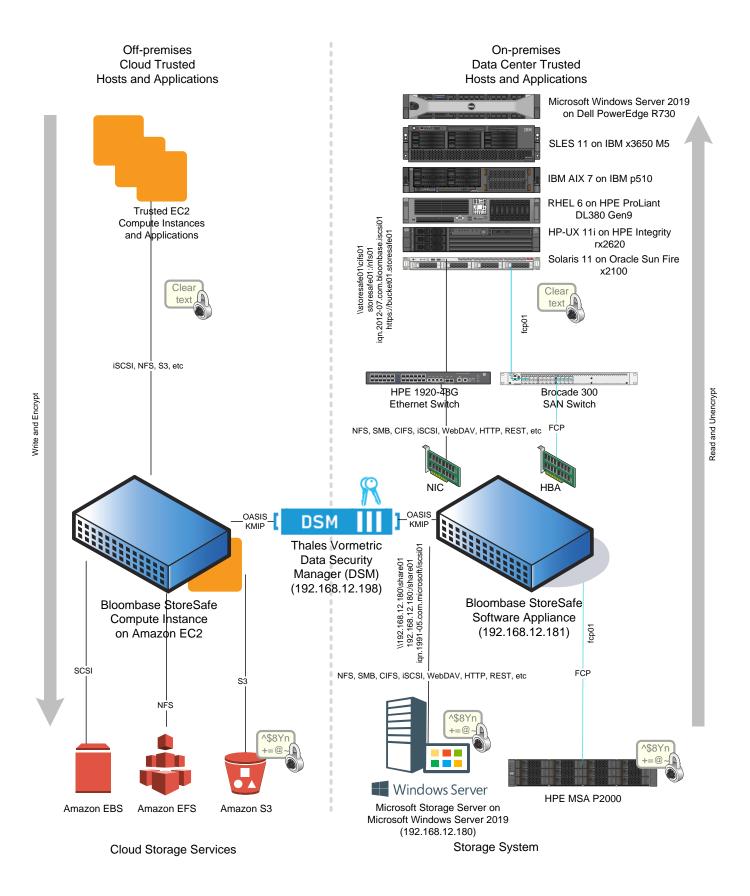
This document describes interoperability testing of Thales Vormetric Data Security Manager (DSM) with Bloombase StoreSafe. Therefore, it is assumed that the reader is familiar with operation of Thales Vormetric Data Security Manager (DSM), storage systems and major operating systems including Linux, 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:



### **Key Management System**

**Key Management System** 

Thales Vormetric Data Security Manager (DSM)

### **On-premises Data-at-Rest Encryption**

Bloombase StoreSafeBloombase StoreSafe Software Appliance v3.4.7HypervisorVMware ESXi 6.0ServerHPE ProLiant DL320eProcessor1x Intel Xeon E3-1220 v3 with AES-NIMemory8 GBNetwork Interface CardOn-board HPE 1GbE NICHost Bus AdapterCavium 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 (S<sub>3</sub>)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic File System (EFS)

### **Client Hosts**

.

Model	Dell PowerEdge	HPE ProLiant	Lenovo System	HPE Integrity	IBM System p5	Oracle Sun Fire
	R730	DL380 Gen9	x3650 M5	rx2620	510	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.

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

THALES Vormetric Data Secur	Log rity Manager Logged in as: mbr Domain: Bloomb:
Dashboard Domains - Administrators - Hosts - Keys	s • Certificates Signatures Policies • Reports Log • System •
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.

THALES	Log Out Logged in as: mbrew Domain: Bloombase		
Dashboard Domains - Adn	ninistrators - Hosts - Keys - Certificates	Signatures Policies - Reports L	.og - System -
🔂 Switch Domains			•
View 20 🔻			Total: 1
Switch to domain			Page 1 of 1
Selected	Domain	Description	
0	Bloombase		
Switch to domain			Page 1 of 1

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

Dashboard Domains - Administrators - Ho			
	sts • Keys • Certificates Signatures	Policies - Repo	rts Log - System -
Edit Host - storesafe.usdev.local			?
General Guard FS Guard VDE Sharing	Host Settings FS/VDE Agent Log K	ey Agent Log Mer	nber
Host Information			
Name storesafe.uso	ev.local	Description	
OS Type Unknown			
FS Communication Port 7024	VDE Commu	ication Port	7025
License Type PERPETUA	_ ▼		
FS Agent Locked	Sys	tem Locked	
Support Challenge & Response	FS Agent One Way Cor	nmunication	
Password Creation Method Generate <b>•</b>	Regenera	te Password	
Secure Start GuardPoint	Supported Encr	ption Mode 🛛 🤇	Offline
Agent Information			
gent Version Certificate Fingerprint	Registration Allowed	Communicat	ion Enabled
5			
ey			
MIP			
		Import	KMIP Cert Ok Apply Cancel

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

THALES Vormetric Data Security Manager								Log Ou Logged in as: mbrev Domain: Bloombase		
Dashboard	Domains - Adn	ninistrators - 🛛	Hosts - Keys	- Certificates	Signatures	Policies -	Reports	Log •	System -	
📃 Imp	port KMIP Client	Certificate							?	)
	KMIP Clien	t Certificate	Choose File	storesafe.cr	t					
									Ok Cance	el

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

т	ΗА	LES	Vormetric Data Securit	y Manager				Log Out Logged in as: mbrew Domain: Bloombase
Dashbo	ard Do	mains - Admin	istrators - Hosts - Keys -	Certificates	Signatures	Policies -	Reports	Log - System -
	Edit Ho	st - storesafe.ı	ısdev.local					?
• St	uccessfully	uploaded self-signed	d client certificate.					
Gen	eral G	uard FS Guard	VDE Sharing Host Settin	igs F5/VDE Ag	ent Log Ke	y Agent Log	Member	
Host	Informat	ion						
		Name	storesafe.usdev.local		[	Description		
		OS Type	Unknown					
	FS Comm	unication Port	7024		VDE Communi	cation Port	7025	
		License Type	PERPETUAL V					
		Agent Locked				em Locked		
	-	je & Response		FS Agent (	One Way Com			
Pa	ssword Cr	eation Method	Generate <		Regenerate	Password		
	Secure Sta	art GuardPoint		Su	pported Encryp	otion Mode	Offline	9
Agent	Informati	ion						
Agent	Version	Certificate Finge	rprint		Regist	ration Allowe	d Com	munication Enabled
S								
(ey								
KMIP	N/A	50:84:09:08:EC:2A	A:E6:55:87:B9:C4:69:1F:30:D4:84:E	35:CB:FF:90				
						[	Import KMIP	P Cert Ok Apply Cancel

## 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.

Storage Management Utility					User: manage Sign Out	<b></b> ↔ <b>63,866,66</b> 11:59:33
System Status           System Time         2018-11-23 06:45:15	Volume demo_0		•			2
System Events 😢 0 🔻 0 🚹 0 🚺 100 Configuration View	View  Provisioning  Volume demo_01 (99.9GB)			Help		
Uninitialized Name (P2000 G3 FC)     Logical	Volume Overvie Details about a specific volume					_
Vdisks	Volume Overview					- All
talaka a wd01 (RAID5)	Component	Count	Capacity	Storage Space		
	<ul> <li>Volume</li> </ul>		100.0GB		100.0GB	
Hosts	Maps	14				
📄 Physical	Schedules	0				
🛕 📙 Enclosure 1	Replication Addresse					
	Replication Images					
	Properties for demo_01					
	Property		Value			
	Vdisk Name		vd01			
	Name		demo_01 99.9GB			
	Size Preferred Owner		99.9GB			
	Current Owner		A			
	Serial Number		00c0ff139da50000a	378f75b0100000		
	Cache Write Policy		write-back			
	Cache Optimization		standard			
	Read Ahead Size		Default			
	Туре		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.

our folder is shared.		
ou can <mark>e-mail</mark> someone links	to these shared items, or <u>copy</u> an	d paste the links into another prog
Individual Items		
share01 \\WIN22-201\share01		
and the second sec	es 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.

lanager							- 0
<ul> <li>Server M</li> </ul>	lanager • File and Storage Se	ervices • iSCSI			• 🕲 I 🧗	<u>M</u> anage <u>T</u> ool	s <u>V</u> iew <u>H</u> elp
Servers Volumes Disks Storage Pools Shares <b>ECS</b> Work Folders	iscsi VIRTUAL DISKS Al SCS virtual disks   1 total Filter Path Status WIN-FNQAP2RH500 (1) CVCCOVirtual/Disks/undisks/seed.shdx			Size m, IGNsign, 1991-05.com, microsoftswinser 184.testad 12.bb.com 200 GB			DASIS •
	Last refreshed on 11/23/2018 2:23:32 AM						_
	C:\iSCSIVirtualDisks\sofsbackend.vhdx on WIN-FN						TASKS 👻
							۲
				stad12 bb.com. ION-inn 1991-05 com microsoftwinser184 testad12 bb.com	-		_
		anna an					
	Server M Servers Volumes Disks Storage Pools Shares ISCSI	Servers Manager * File and Storage So Servers Volumes Disks Shares KCSI Work Folders Work Folders CSI CyCS/Virtual/Disks/cofbackerd.vbdc on WIN-FN Filer CyCS/Virtual/Disks/cofbackerd.vbdc on WIN-FN Filer Name Server Name Target (DA	Server Manager + File and Storage Services + iSCSI  Servers Volumes Disks Shares KCS Work Folders Virtual Disk Status Vir	Server Manager • File and Storage Services • iSCSI Servers Volumes Disks Storage Pools Shares KCS Volume Target Name Target Status Initiator ID Target Status Initiator ID Target Status Initiator ID Target Status Target Status Initiator ID Target Status Initiator ID	Server Manager + File and Storage Services + iSCSI         Servers         Volumes         Disks         Storage Pools         Work Folders         Work Folders         Storage Pools         Storage Pools	Server Manager + File and Storage Services + iSCSI       • ② I *         Servers       Marco Site With a Goog 1 to all         Volume       D • ③ • ④ • ①         Sorage Pools       An SCSI With a Goog 1 to all         Volume       D • ④ • ④ • ①         Volume       D • ④ • ① • ① • ① • ① • ① • ① • ① • ① • ①	Server Manager + File and Storage Services + iSCSI       • ② I * More too         Server Sources       Sign MRTUAL DESS         Volumes       Image: P ima

Х

### **Amazon EFS Cloud Storage Services**

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

aws	Service	s.≁	Reso	urce Gro	ups 🗸 🍾	¢	michael.brew @ 4370-6154-16	🕶 N. California 👻	Support 👻
File systems	•		syste	ems system	Actions -				<b>२</b>
				Name	File system ID	Metered size	Number of mount targets	Creation date	
		۲	•		fs-cb6385d2	20.0 KiB	1	05/29/2018, 09:22:4	7 UTC
Feedback	🖸 Englis	h (US)			© 2	008 - 2018 Amazon We	h Services. Inc. or its affiliates. All rights r	eserved Privacy Policy	Term

### **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).

vmware <sup>®</sup> vSphere Web Cli	ent ते≡ Ù   michael.brew@US.BLOOMBASE.COM -   Help -   Q Search
Navigator I	🔂 Interop Store Safe 3.4.7.1 (22.39) Actions 👻 🔁 Alarms
Home 🕨 🔊	Getting Started Summary Monitor Manage Related Objects All (0) New (0)
Home	Getting Started       Summary       Monitor       Manage       Related Objects       All (0)       New (0)         Interop Store Safe 3.4.7.1 (22.39)       Guest OS:       Red Hat Enterprise       CPU USAC         Guest OS:       Red Hat Enterprise       Interop Store Safe 3.4.7.1 (26.39)       CPU USAC         Guest OS:       Red Hat Enterprise       Interop Store Safe 3.4.7.1 (26.39)       MEMORY         Compatibility:       ESX 6.0 and later (VM       WEXARY       20.00 M         Version 11)       VMw are Tools:       20.47483647 (Guest       STORAGE         VIEW are Tools:       2147483647 (Guest       Managed)       STORAGE         DNS Name:       storesafe.usdev.local       IP Addresses:       192.168.22.39         View all 3 IP addresses       Host:       192.168.22.20       11
🔂 k8s03	► VM Hardware
<ul> <li>StoreSafe 3.4.7.1 (</li> <li>StoreSafe 3.4.7.1 (</li> <li>StoreSafe 3.4.7.2</li> <li>Win10 (22.50)</li> <li>Win10 (22.51)</li> <li>Win7 office2007</li> <li>Windows 10 Remote 2</li> <li>Windows 2012 bbdc01</li> <li>Windows 2012 R2 usd</li> <li>Windows 2016 (22.201)</li> </ul>	<ul> <li>Advanced Configuration</li> <li>Notes</li> <li>Tags         <ul> <li>Assigned Tag</li> <li>Catego</li> <li>This lie</li> </ul> </li> <li>vApp Details</li> <li>::</li> </ul>
😴 Recent Tasks	
Task Name	Target     Status     Initiator     Queued For     Start Time       Image: Status     Image: Status     Image: Status     Image: Status     Image: Status       Image: Status     Image: Status     Image: Status     Image: Status     Image: Status       Image: Status     Image: Status     Image: Status     Image: Status     Image: Status       Image: Status     Image: Status     Image: Status     Image: Status     Image: Status       Image: Status     Image: Status     Image: Status     Image: Status     Image: Status       Image: Status     Image: Status     Image: Status     Image: Status     Image: Status       Image: Status     Image: Status     Image: Status     Image: Status     Image: Status       Image: Status     Image: Status     Image: Status     Image: Status     Image: Status       Image: Status     Image: Status     Image: Status     Image: Status     Image: Status       Image: Status     Image: Status     Image: Status     Image: Status     Image: Status       Image: Status     Image: Status     Image: Status     Image: Status     Image: Status       Image: Status     Image: Status     Image: Status     Image: Status     Image: Status       Image: Status     Image: Status     Image: Status     Image: Status
My Tasks ▼ Tasks Filter ▼	

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".

🏠 Main 🔶 Logout	e s	upport 📑 Al	bout 🤗 Help	)			
<b>B</b> Bloombase	Stor	reSafe Sec	curity Ser	ver			
<b>Greeting</b> Host Name: storesafe01		List K	MIP Key	Manager			
User: admin Datetime: 2016-05-12 01:32:40 +0200		List KMI	P Key Man	ager			
		2	Name	Model	Но	st Address	Port
Menu Bar					Add		
System	$\sim$				Add		
Operation	$\sim$						
Network Security	$\sim$						
High Availability	$\sim$						
Administration	$\sim$						
Key Management	$\sim$						
Bloombase KeyCastle							
Hardware Security Module							
OASIS KMIP Key Manager							
Find Key Wrapper							
Create Key Wrapper							
StoreSafe Configurations	$\sim$						
Storage	$\sim$						
Language							
English 🔻							
Copyright © 2016 Bloombase							

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".

		eSafe Securit	J			
Greeting		Modifu Kl	MIP Key Mo	ınaaer		
lost Name: toresafe.usdev.local		55512	5-12			
Iser: admin		Modify KMTP	Key Manager			
atetime: 2018-11-07 1:08:35 -0800						
1.08.33 -0800		Name	ThalesPartnerTestDS			
enu Bar		Model	Vormetric DSM	•		
stem		Host Addresses	;i			
peration		Port	5696			
		Timeout	30000	ms		
etwork Security	× ·	Retry Count	1			
igh Availability	~	Retry Wait Time	3000	ms		
Iministration	~	Username				
ey Management	^	Password				
oombase KeyCastle			Test Sul	mit Refresh	Delete Cancel	
rdware Security Module						
SIS KMIP Key Manager						
oud Key Managers		Client Keysto	ore			
nd Key Wrapper		Key Bit Length	2048 🔻			
eate Key Wrapper oreSafe Configurations	~	Signature Hash	SHA256 V			
	Ŭ	Country	US			
orage	~	State	CA			
anguage		Locality				
English V		Organization	Bloombase			
English .		Organizational Unit	t (			
		Common Name	storesafe.usdev.l	ocal		
Copyright © 2018 Bloombase		Generate	Cancel			
		denerate				
		Trust Certific	cate			
		Subject Name				
		Serial Number				
		Issuer Name				
		Valid Start Date				
		Valid End Date				

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.

Network Security     V     Retry Count     1       High Availability     V     Retry Wait Time     3000     ms       Administration     V     Username     V	
High Availability Y Retry Wait Time 3000 ms	
Key Management  A Password	
Bloombase KeyCastle Test Results :	
Hardware Security Module 12.104.149.25 : Success Vendor ID : Vormetric	
OASIS KMIP Key Manager	
Cloud Key Managers (Test) Submit (Refresh) Delete Cancel	
Find Key Wrapper	
Create Key Wrapper Client Keystore	
StoreSafe Configurations V CN=storesafe.usdev.local	
Storage  Subject Name Subject Name Subject Name Str=CA C=US	
Language Serial Number 00cd2aeaae33538cbe8306	
English ▼ CN=storesafe.usdev.local Issuer Name CN=storesafe.usdev.local O=Bloombase ST=CA C=US	
Copyright © 2018 Certificate 🐻	
Bloombase Valid Start Date 2018-11-07	
Valid End Date 2023-11-07	
Create Certificate Request	
Client Key/ Certificate Choose File No file chosen	
Pin	
Trust Certificate	
C=US ST=CA L=San Jose O=Thales eSecurity OU=Business Development CN=CG CA S on ThalesPartnerTestDSM	
Serial Number 00b3a2106a17	
C=US         ST=CA         Issuer Name       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 Upload	
	-

Click 'Submit' to commit the configuration. If the certificates are setup properly, "test results" of the KMIP Key Manager would return "Success".

Lis	st I	KMIP Key Manager			
List	t KN	1IP Key Manager			
	2	Name	Model	Host Address	Port
	1	ThalesPartnerTestDSM	Vormetric DSM	12.104.149.25	5696
			Add		

#### **Encryption Key Provisioning**

Generate encryption key with name  ${\tt key01}$  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".

🗥 Main <⊱ Logout	🤤 Si	upport	A	Abou	t 🏆 Helj	D								
<b>B</b> Bloombase	Stor	reSaf	ie S	Secu	rity Ser	ver								
Greeting Host Name: storesafe01 User: admin Datetime: 2017-01-18 11:24:17 -0800		<b>Fir</b> Nar	nd me		y Wraj Vrapper		Туре			▼ Act	tive	▼ c	A	•
Menu Bar		~	MOR	e option	5									
System	$\sim$							Find		Reset	Add			
Operation	$\sim$													
Network Security	$\sim$													1-1 of 1
High Availability	$\sim$		2	Name	Туре	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
Administration	$\sim$		1	kev01	Symmetric	KMIP	<b>V</b>			UUID=02-	KMIP=DSM			2017-01-18
Key Management	~				-,					73				09:57:25 -0800
Bloombase KeyCastle														1-1 of 1 🖸 🔽
Hardware Security Module														
OASIS KMIP Key Manager														
Find Key Wrapper														
Create Key Wrapper														
StoreSafe Configurations	$\sim$													
Storage	$\sim$													
Language														
English V														
Copyright © 2017 Bloombase														

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

Key Wrap	per Permissions			
Modify Ke	y Wrapper			
Key Source	OASIS KMIP Key Mana	iger 🔻		
Key Manager	ThalesPartnerTestDSM	•		
Object			T	
		Select Key	Add Key	
		Clo		

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'.

Key Wrapper	Permissions	
lodify Key Wr	apper	
Name	key01	
Key Source	OASIS KMIP Key Manager	
Гуре	Symmetric	
Active		
KMIP Key Manager	ThalesPartnerTestDSM	
MIP UUID		
KMIP Key Name		
KMIP Key State		
Key Bit Length	256 🔻	
Dwner	admin	
Last Update Datetime		
	Generate	
	(Submit) Close	

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

тн	ALES	Vormetr	ic Data S	Security	y Manager					Log Jed in as: mb nain: Bloomb	
Dashboard	Domains - Admin	istrators -	Hosts -	Keys -	Certificates	Signatures	Policies	- Repo	rts Log-	System -	
🤌 кмі	IP Objects										?
										Hide Sea	rch
KMIP Ob	ojects										
	UUID ation Date (From) reation Date (To)						Type State		<b>T</b>	Tota	Go I: 9
									Page 1 of	1 🖪 🗖 🕨	ÞI
Name	Unique Identifie				State			reation Ti			
	714c2acb-a00d-44				Active				7:41:20 PST 20		
1	16f18bab-67d7-4b				Active		-		7:41:20 PST 20		
key01	5894bb45-1e36-41 f46f6770-884e-4ae				Active				7:41:19 PST 20 1:53:27 PST 20		
	13a9d610-68a2-43				Active		-		1:53:27 PST 20 1:53:27 PST 20		
kl-test-kev01	ca3fdcce-a342-462				Active				1:53:27 PST 20 1:53:27 PST 20		
KI-LESL-KEYUI	2290531b-6a9a-40				Active				14:06:25 PST 2		
	45d5c5c7-fd68-41				Active		-		14:06:24 PST 2		
jw-test-key01	88fbf7fd-e50d-435				Active	e SymmetricK	ey T	hu Nov 15	14:06:22 PST 2	018	
									Page 1 of	1 🖪 🗖 🕨	ÞI

#### **Backend Physical Storage Configuration**

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

Physical Storage	Permissions		
hysical Storage	e Configuration		
Name	share01		
Description			
Physical Storage Type	Pass Through 🔻		
lost	win22-201.usdev.local		
Share Name	share01		
Domain	usdev.local		
VTLMv1			
Vetapp			
/irtual Storage			
Dwner	admin		
ast Update Datetime			
		Submit Close	

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

Physical Storage	Permissions
Physical Storag	e Configuration
Name	EFS
Description	
Physical Storage Type	Remote v
Гуре	Network File System (NFS)
lost	172.31.32.253
Share Name	
Read Size	
Vrite Size	
Synchronous	
lount Hard	
ptions	
/irtual Storage	EFS
)wner	admin
ast Update Datetime	2017-01-12 02:58:06 -0500
	Submit Delete Close

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

Modify Stora	ge Configuration
Physical Storage	Permissions
Physical Storage	Configuration
Name	lun01
Description	
Physical Storage Type	Device
Туре	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
	Submit Delete Close

 $i SCSI \ physical \ storage \ namely \ \texttt{iscsi01} \ is \ configured \ to \ be \ secured \ by \ Bloombase \ StoreSafe \ using \ encryption.$ 

Physical Storage	Permissions
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
	Submit Delete Close

#### 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.

ot secure   https://19	92.168.22.39:8443/	ActionServlet			
Modify Virtı	ıal Storage	2			
Virtual Storage	Protection	Access Control	Permissions		
Aodify Virtual S	torage				
Name	share01				
Description					
Active			_10		
Mode	File •				
Protocol	SMB V				
Owner	admin				
ast Update Datetime					
Settings					
Offline Setting Disal	bled <b>v</b>				
Physical Storage	e				
Storage	share01 🔑 📆				
	📱 Please input st	orage			
Description					
Physical Storage Type	Pass Through				
Host	win22-201.usdev.l	lean			

Modify Virt	ual Storag	<i>je</i>	
Virtual Storage	Protection	Access Control	Permissions
Modify Virtual S	Storage		
Name	EFS		
Status			
Description			
Active			
Mode	File		
Owner	admin		
Last Update Datetime	2017-01-12 03:	51:52 -0500	
Settings			
Offline Setting Disa	abled 🔻		
Physical Storag	e		
Storage	EFS P 🕅		
Description			
Physical Storage Type	Remote		
		Submit Delete	Status Close

Modify Virtu	al Storag	е		
Virtual Storage	Protection	Access Control	Permissions	
Modify Virtual St	orage			
Name	san01			
Status				
Description			le le	
Active				
Mode	FC 💌			
Owner	admin			
Last Update Datetime	2011-02-19 02:4	l6:25 +0800		
Physical Storage				
Storage	lun01 🔑 😿			
Description				
Physical Storage Type	Device			
	Sul	bmit Delete (	Close	

Virtual Storage	Protection	Access Control	iSCSI	Permissions
lodify Virtual S	Storage			
ame	iqn.2016-11.com.	bloombase.iscsi:targ	et	
Status				
escription				
Active	•			
1ode	iSCSI			
ape Library				
ATS				
Cluster				
/endor	BLOOMBASE			
1odel	VIRT-SCSI			
Revision				
Dwner	admin			
ast Update Datetime Physical Storag		:39 -0700		
A Stor	age Description			Device
1 iscsi01		4f504e46494c455	274646f435	i8622d477248772d39704768

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 Securi	ity Server - Web Mana	agement Console - Go	ogle Chrome		-	×
A Not secure   https://1	92.168.22.39:8443,	/ActionServlet				
Modify Virta	ual Storage	e Handler Access Control	Permissions			
	vacy 🔻					
Encryption Keys	5 Key Nan key01	ne	Last Up	date Datetime		
		Add	Remove			
Header Protected						
Cryptographic C	Cipher					
	56 V					
CTR Mode 🖉	)	Submit	Close			
https://192.168.22.39:8443/Actic	onServlet#					

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.

ot secure	e   <del>htt</del>	<del>:ps</del> ://192.168.22.39:84	143/ActionServlet				×
Virtu	al Stor	age Protection	Access Control	Permissions			
Default		Read Write	ectory (MSAD) 🔻				
윋			User	Access Control List	Last Update Datetime	a	
1			•	🗹 Read 🗹 Write			
∨ More (	Options	Group: Domain Users ususer01@USDEV.LOO ususer02@USDEV.LOO ususer03@USDEV.LOO	@USDEV.LOCAL	Remove			
	Default User Rep	ot secure htt Modify V Virtual Stor User Access Default User Repository	ot secure https://192.168.22.39:84 Modify Virtual Stored Virtual Storage Protection User Access Control Default Read Write User Repository Microsoft Active Dir 1 □ Group: DEV@USDEV.LO Group: DEV@USDEV.LO Ususer01@USDEV.LO Ususer03@USDEV.LO	ot secure https://192.168.22.39:8443/ActionServlet   Modify Virtual Storage Access Control   Virtual Storage Protection   Access Control   Default Read   Wirte   User Repository Microsoft Active Directory (MSAD)       I   Croup: DEV@USDEV.LOCAL    Group: DEV@USDEV.LOCAL    Wore Options   ususer01@USDEV.LOCAL   User 01	Modify Virtual Storage Access Control         Virtual Storage       Protection       Access Control       Permissions         User Access Control         Default       Read       Write         User Repository       Microsoft Active Directory (MSAD) <ul> <li>Image: State Control List</li> <li>Image: State Control List</li></ul>	ot secure https://192.168.22.39:8443/ActionServlet   Modify Virtual Storage Access Control Virtual Storage Protection Access Control Default Read Write User Repository Microsoft Active Directory (MSAD) Virtual Storage Control List Last Update Datetime I Group: DEV@USDEV.LOCAL Group: DEV@USDEV.LOCAL Ususer03@USDEV.LOCAL USUSER0	bot secure https://192.168.22.39:8443/ActionServlet   Modify Virtual Storage Access Control   Virtual Storage Protection   Access Control Default   Read Write   User   Access Control List Last Update Datetime     1 Virtual Storage USDEV.LOCAL   More Options   Ususer02@USDEV.LOCAL     Ususer02@USDEV.LOCAL   Wore Options   Ususer02@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/vormetricdata-security-manager
- 5. HPE P2000 MSA, https://support.hpe.com/hpsc/doc/public/display?docId=emr\_na-co2020084
- 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 (S<sub>3</sub>), https://aws.amazon.com/s<sub>3</sub>/
- 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/networkingswitches/pip.switches.7399514.html
- 12. OASIS Key Management Interoperability Protocol (KMIP), https://www.oasis-open.org/committees/kmip/