Executive Summary

HashiCorp Vault has been validated by Bloombase InteropLab to run with Bloombase StoreSafe Intelligent Storage Firewall. This document describes the steps carried out to integrate HashiCorp Vault with Bloombase StoreSafe software appliance on VMware ESXi to deliver high bandwidth transparent storage encryption for mission critical applications. Client host system Microsoft Windows 11 has been tested with HashiCorp Vault and Bloombase StoreSafe data-at-rest encryption solution to secure Microsoft Storage Server 2022 storage backend.
Table of Contents
Table of Contents

Purpose and Scope 5

Assumptions 6

Infrastructure 7
Setup 7
Key Management 9
Storage Encryption 9
Storage System 9
Application Client 9

Configuration Overview 10
HashiCorp Vault 10
HashiCorp Vault Configurations 10
HashiCorp Vault Client Enrollment 12
Microsoft Storage Server on Microsoft Windows Server 2022 13
SMB Services Configuration 14
NFS Services Configuration 16
iSCSI Services Configuration 18
Bloombase StoreSafe Intelligent Storage Firewall 18
HashiCorp Vault and Bloombase StoreSafe Integration 19
Encryption Key Provisioning 21
Data-at-Rest Encryption for SMB 24
Data-at-Rest Encryption for NFS 28
Data-at-Rest Encryption for iSCSI 32

Use Cases 37
Data-at-Rest Encryption for SMB 37
Data-at-Rest Encryption for NFS 40
Data-at-Rest Encryption for iSCSI 45

Conclusion 52

Disclaimer 54

Acknowledgement 55

Reference 56
Purpose and Scope

This document describes the steps necessary to integrate HashiCorp Vault with Bloombase StoreSafe to deliver agentless, transparent encryption security of traditional storage systems and next-generation storage services for mission-critical applications. Specifically, we cover the following topics:

- Install and configure Bloombase StoreSafe software appliance
- Integrate Bloombase StoreSafe with HashiCorp Vault
- Integrate application components Microsoft Windows 11 client host system and Microsoft Storage Server 2022 with Bloombase StoreSafe and HashiCorp Vault to demonstrate how high-bandwidth, agentless, application-transparent data encryption could be achieved for multiple network storage protocols namely SMB, NFS and iSCSI
Assumptions

This document describes the integration of HashiCorp Vault with Bloombase StoreSafe. It is assumed that you are familiar with operation of HashiCorp Vault, storage systems, and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is also assumed that you possess basic UNIX administration skills. The examples provided may require modifications before they are run under your version of operating system.

As HashiCorp Vault is third party option to Bloombase StoreSafe data at-rest encryption security solution, you are recommended to refer to installation and configuration guides of specific model of HashiCorp Vault for your actual use cases. We assume you have 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://support.bloombase.com.
Infrastructure

Setup

The integration discussed in this guide is based on the system block diagram below:
Microsoft Windows 11

```
\bloombase\smb01
bloombase/nfs01
iqn.2012-07.com.bloombase:iscsi01
```

NFS, SMB, CIFS, iSCSI, FCP, NVMe-oF, WebDav, HTTP, REST, S3, etc

Bloombase StoreSafe

```
\storage01\smb01
storage01/nfs01
iqn.1991-05.com.microsoft:iscsi01
```

NFS, SMB, CIFS, iSCSI, FCP, NVMe-oF, WebDav, HTTP, REST, S3, etc

Microsoft Storage Server on Microsoft Windows Server 2022

HashiCorp Vault Enterprise

```
^$8Yn
+=@~
```

KMIP

Clear text

Write and Encrypt

Read and Unencrypt
## Key Management

| Key Manager | HashiCorp Vault 1.8.3+ent |

## Storage Encryption

<table>
<thead>
<tr>
<th>Storage Encryption</th>
<th>Bloombase StoreSafe Intelligent Storage Firewall Software Appliance v3.4.8.4-EA2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>VMware Virtual Machine (VM) on VMware ESXi 6.5</td>
</tr>
<tr>
<td>Processor</td>
<td>4 x Virtual CPU (vCPU)</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
</tr>
</tbody>
</table>

## Storage System

| Storage System | Microsoft Storage Server on Microsoft Windows Server 2022 on VMware ESXi 6.5 |

## Application Client

| Client Host | Microsoft Windows 11 on VMware ESXi 6.5 |

Configuration Overview

HashiCorp Vault

HashiCorp Vault is an identity-based secrets and encryption management system. Vault provides encryption services that are gated by authentication and authorization methods. Arbitrary key/value secrets can be stored in Vault. Vault encrypts these secrets prior to writing them to persistent storage, so gaining access to the raw storage isn’t enough to access your secrets.

The HashiCorp Vault provides central management and secure storage of encryption keys, including those generated by Bloombase StoreSafe products, and KMIP-compliant cloud vendors. It provides intuitive web-based console, and APIs for managing of encryption keys.

The KMIP services provided by HashiCorp Vault are used by Bloombase StoreSafe for encryption protection of data-at-rest use cases.

HashiCorp Vault Configurations

Assume HashiCorp Vault is installed and configured as a network attached appliance with IP address

192.168.23.131
HashiCorp Vault can be managed remotely via CLI-based text console at address:

https://192.168.23.131:8200

Alternatively, the web dashboard of the HashiCorp Vault can be accessed at the same address:

https://192.168.23.131:8200
HashiCorp Vault Client Enrollment

To establish the trust and allow communication between HashiCorp Vault and Bloombase StoreSafe, certificates need to be created and stored in the HashiCorp Vault and the Bloombase StoreSafe. In the HashiCorp Vault, this can be configured as follows.

Enable the KMIP feature, with the network address, and other configurations. For example:

```bash
vault secrets enable kmip
vault write kmip/config listen_addrs=0.0.0.0:5696
    server_ips="192.168.23.131"
    tls_ca_key_type="rsa"
    tls_ca_key_bits=2048
    default_tls_client_key_type="rsa"
    default_tls_client_key_bits=2048
```

Create a scope and role:

```bash
vault write -f kmip/scope/bloombase
vault write kmip/scope/bloombase/role/admin operation_all=true
```

An example configuration can be seen in the figure below:
KMIP client certificate and key is generated and downloaded from HashiCorp Vault. Download the Certificate and upload to the Bloombase StoreSafe trusted client configuration.

Note, you are required to convert the JSON format (key and certificate) to PKCS #12 format in order to upload to the Bloombase StoreSafe.

```
vault write -format=json kmip/scope/bloombase/role/admin/credential/generate format=pem > vault_credential.json
```

Also, download the HashiCorp Vault CA certificate which will be needed to be imported to the trusted server configuration at the Bloombase StoreSafe

```
vault read kmip/ca
```

**Microsoft Storage Server on Microsoft Windows Server 2022**

Microsoft Storage Server on Microsoft Windows Server 2022 running on VMware ESXi is used in this interoperability test which is able to provide storage services over network storage protocols including NVMe-oF, FCP, iSCSI, NFS, SMB, CIFS, REST, etc.

Microsoft Windows Server 2022 is deployed as a virtual machine (VM) on VMware ESXi.
SMB Services Configuration
Microsoft Windows Server 2022 File Management is configured to provide the SMB share backend storage to client system users.
NFS Services Configuration
NFS storage service is provisioned on Microsoft Windows Server 2022 to be used in this integration testing.
iSCSI Services Configuration

iSCSI storage service is also provisioned on Microsoft Windows Server 2022 to be used in this integration testing.

Bloombase StoreSafe Intelligent Storage Firewall

Bloombase StoreSafe delivers unified data at-rest encryption security of files, block devices, objects, sequential storages, etc. In this interoperability test, both file-based and block-based encryption security services are validated against Bloombase StoreSafe with keys managed at HashiCorp Vault.

Bloombase StoreSafe Intelligent Storage Firewall software appliance is deployed as a virtual appliance (VA) on VMware ESXi.
HashiCorp Vault and Bloombase StoreSafe Integration

Bloombase StoreSafe Intelligent Storage Firewall supports HashiCorp Vault 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 HashiCorp Vault, the KMIP service configuration at Bloombase web management console has to be set up.

First of all, import HashiCorp Vault’s X.509 client key pair as “Client Keystore” and server certificate into “Trust Certificate” at the Bloombase StoreSafe web management console so as to establish the trust between Bloombase StoreSafe and HashiCorp Vault.
Next, add the HashiCorp Vault instance to the Bloombase StoreSafe KMIP configuration. This is done by clicking “OASIS KMIP Key Manager” under “Key Management”.

Input a name for the HashiCorp Vault

```plaintext
vault01
```

and select Model as

```plaintext
HashiCorp Vault
```

Input also the host name

```plaintext
vault01
```
or IP address

192.168.23.131

and KMIP service port

5696

to access the HashiCorp Vault.

Click 'Submit' to commit the configuration. If the certificates are setup properly, “Test Results” of the KMIP Key Manager would return “Success”.

Encryption Key Provisioning

To generate key in attached HashiCorp Vault, select Key Source Type as

OASIS KMIP Key Manager

and the assigned Key Manager label, in this case

vault01

Select “Add Key” and “generate” to create a new key on the HSM.
Or if key already exists, simply choose from the dropdown box.
Ensure that you import a key from the KMIP key manager before you submit the key wrapper at Bloombase StoreSafe.

Cross check at the HashiCorp Vault console that the newly generated key can be found on the HashiCorp Vault server.
Data-at-Rest Encryption for SMB

Physical storage namely

smb01

is configured to be secured by Bloombase StoreSafe using encryption.
Virtual storage namely

smb01

of type

File

is created to virtualize physical storage

smb01

for application transparent encryption protection over network file protocols including CIFS.
Protection type is specified as Privacy and secure the Microsoft Storage Server storage backend using AES 256-bit encryption and encryption key key01 managed at HashiCorp Vault.
SMB/CIFS storage protocol relies mainly on user-password authentication for access control. In this test, the Bloombase StoreSafe secure storage resource `smb01` is provisioned for user `user01` with Microsoft Active Directory integration for user-password authentication and single sign-on.
Data-at-Rest Encryption for NFS

Physical storage namely

nfs01

is configured to be secured by Bloombase StoreSafe using encryption.
Virtual storage namely nfs01 of type File is created to virtualize physical storage nfs01 for application transparent encryption protection over network file protocols including NFS.
Protection type is specified as Privacy and secure the Microsoft Storage Server storage backend using AES 256-bit encryption and encryption key key01 managed at HashiCorp Vault.
NFS storage protocol relies mainly on UID/GID and networking for access control. In this test, the Bloombase StoreSafe secure storage resource

nfs01

is provisioned for client IP

192.168.12.242
Data-at-Rest Encryption for iSCSI

Physical storage namely

iscsi01
is configured to be secured by Bloombase StoreSafe using encryption.

### Modify Storage Configuration

<table>
<thead>
<tr>
<th>Physical Storage Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Physical Storage Type</td>
</tr>
<tr>
<td>Block I/O</td>
</tr>
<tr>
<td>Multipath</td>
</tr>
<tr>
<td>Device ID (max 8 chars)</td>
</tr>
<tr>
<td>Options</td>
</tr>
<tr>
<td>Device</td>
</tr>
<tr>
<td>Virtual Storage</td>
</tr>
<tr>
<td>Owner</td>
</tr>
<tr>
<td>Last Update Datetime</td>
</tr>
</tbody>
</table>

Virtual storage namely

`ign.2012-07.com.bloombase:iscsi01`

of type

`iSCSI`

is created to virtualize physical storage

`iscsi01`

for application transparent encryption protection over network file protocols including iSCSI.
Protection type is specified as

Privacy

and secure the Microsoft Storage Server storage backend using

AES XTS 256-bit

encryption and encryption key

key01

managed at HashiCorp Vault.
iSCSI storage protocol relies mainly on CHAP, IQN, and networking for access control. In this test, the Bloombase StoreSafe secure storage resource

```
ign.2012-07.com.bloombase:iscsi01
```

is provisioned for initiator

```
ign.1991-05.com.microsoft:window11
```
Modify Virtual Storage Access Control

**Allowed Portal**

<table>
<thead>
<tr>
<th>Portal IP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

- Add
- Remove

**Incoming Users**

<table>
<thead>
<tr>
<th>User</th>
<th>Warning</th>
<th>Last Update Datetime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Add
- Remove

**Initiators**

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Alias</th>
<th>Warning</th>
<th>Last Update Datetime</th>
</tr>
</thead>
</table>

- Add
- Remove

List initiators

Refresh Alias Submit Close
Use Cases

Data-at-Rest Encryption for SMB

SMB shares are an example from the many protocols Bloombase StoreSafe supports for encryption. A share from a Windows Server 2022 system that is accessible by domain users is created to act as backend storage. Bloombase StoreSafe creates a virtual encrypted share on its own hostname path that is accessed from a client software system.
Windows 11 clients can use the included network share on file manager to access the SMB share. Data owners can alternatively use the Net Use command to specify additional mounting options.
On the demo virtual encrypted SMB share, a sample plaintext file is created by the client and saved. The file is transparently encrypted by the Bloombase StoreSafe encryption engine and stored on the Windows Server 2022 backend share.

If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.
Data-at-Rest Encryption for NFS

NFS shares are an example from the many protocols Bloombase StoreSafe supports for encryption. A share from a Windows Server 2022 system that is accessible by configure clients is created to act as backend storage. Bloombase StoreSafe creates a virtual encrypted share on its own hostname path that is accessed from a client software system.
Windows 11 clients can use the included map network drive option to add the NFS share with a drive letter. Data owners can alternatively use the mount command to specify additional mounting options.
On the demo virtual encrypted NFS share, a sample plaintext file is created by the client and saved. The file is transparently encrypted by the Bloombase StoreSafe encryption engine and stored on the Windows Server 2022 backend share.
If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.
Data-at-Rest Encryption for iSCSI

iSCSI targets are an example from the many protocols Bloombase StoreSafe supports for encryption. A target from a Windows Server 2022 system that is accessible by configure clients is created to act as backend storage. Bloombase StoreSafe creates a virtual encrypted share on its own hostname path that is accessed from a client software system.
Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

**IP address or DNS name:** bloombase01

**Port:** (Default is 3260)

3260

Advanced... OK Cancel

iSNS servers

The system is registered on the following iSNS servers:

Name

Refresh

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click Remove.
Windows 11 clients can attach the virtual encrypted share with the default iSCSI initiator tool. Add the hostname and port to the discover tab, then connect to the Bloombase StoreSafe target. To access the iSCSI disk, make sure the client IQN is be added the Bloombase StoreSafe configuration. The disk will be mounted to the system and it can be formatted with a filesystem.
On the demo virtual encrypted iSCSI target, a sample plaintext file is created by the client and saved. The file is transparently encrypted by the Bloombase StoreSafe encryption engine and stored on the Windows Server 2022 backend target.
If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.
Conclusion

In this integration guide, we have shown how to set up Bloombase StoreSafe Intelligent Storage Firewall with HashiCorp Vault to deliver on-the-fly encryption of multiple storage protocols including SMB, NFS and iSCSI. The end result is a high-bandwidth, application-transparent storage encryption solution with centralized key management that locks down sensitive crown-jewel data on disks and helps mitigate information exfiltration threats for mission-critical systems and data services.

As a summary,

- HashiCorp Vault

has been integrated with Bloombase StoreSafe Intelligent Storage Firewall to deliver encryption security of Microsoft Storage Server on Microsoft Windows Server 2022 over SMB/CIFS, NFS and iSCSI network storage protocols for software applications running on Microsoft Windows Server 2022 and Windows 11.

<table>
<thead>
<tr>
<th>Bloombase Product</th>
<th>Application Components</th>
<th>Key Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bloombase StoreSafe Intelligent Storage Firewall</td>
<td>• Microsoft Storage Server</td>
<td>• HashiCorp Vault 1.8.3+ent</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2022</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows 11</td>
<td></td>
</tr>
</tbody>
</table>
Disclaimer

The integration procedures 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 difference 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 HashiCorp team for supporting the integration of Bloombase StoreSafe with HashiCorp Vault.
Reference

2. Bloombase StoreSafe Hardware Compatibility Matrix, https://www.bloombase.com/content/e8Gzz281