

BLOOMBASE CONFIDENTIAL



Bloombase InteropLab – Use Cases and Certification: Bloombase StoreSafe and VMware Cloud on Amazon Web Services (VMC on AWS)



This document contains information of a proprietary nature. **ALL INFORMATION CONTAINED HEREIN SHALL BE KEPT IN CONFIDENCE.** None of this information shall be divulged to persons other than Bloombase employees authorized by the nature of their duties to receive such information, or individuals or organizations authorized by Bloombase research and development in accordance with existing policy regarding the release of company information

BLOOMBASE CONFIDENTIAL

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, Spitfire, StoreSafe are either registered trademarks or trademarks of Bloombase in the United States, Canada, European Union and/or other countries.

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

Document No.: Bloombase InteropLab - Interoperability and Certification - Use Cases and Certification – Bloombase StoreSafe and VMware Cloud on Amazon Web Services (VMC on AWS) - vo.g1.doc

BLOOMBASE CONFIDENTIAL

Table of Contents

1. Document Revision History	5
2. Introduction	6
2.1 Use Cases for VMware Cloud on AWS	10
2.1.1 Bloomberg StoreSafe deployment by OVF	10
2.1.2 Bloomberg StoreSafe deployment by vMotion	11
2.1.3 Bloomberg StoreSafe text console	11
2.1.4 Bloomberg StoreSafe web management console	11
2.2 Use Cases for Amazon CloudHSM	11
2.2.1 Bloomberg StoreSafe integration with Amazon CloudHSM for centralized lifecycle key management	12
2.3 Use Cases for Amazon Elastic File System (EFS)	12
2.3.1 Bloomberg StoreSafe NFS virtual storage with host network access control	13
2.3.2 Bloomberg StoreSafe NFS virtual storage	14
2.3.3 Bloomberg StoreSafe NFS virtual storage network share connection	14
2.3.4 Mount Bloomberg StoreSafe NFS virtual storage	14
2.3.5 Store and encrypt contents at Bloomberg StoreSafe NFS virtual storage via mount point	14
2.3.6 Retrieve and un-encrypt contents at Bloomberg StoreSafe NFS virtual storage via local file system	15
2.4 Use Cases for Amazon Simple Storage Service (S3)	15
2.4.1 Bloomberg StoreSafe S3 virtual storage with access control	16
2.4.2 Bloomberg StoreSafe S3 virtual storage	17
2.4.3 Bloomberg StoreSafe S3 virtual storage network share connection	17
2.4.4 Store and encrypt contents at Bloomberg StoreSafe S3 virtual storage	17
2.4.5 Retrieve and un-encrypt contents at Bloomberg StoreSafe S3 virtual storage	17
2.5 The Bloomberg Solution Configuration Screens	18
2.5.1 Installation	18
2.5.2 Management	19
3. Bloomberg Interoperability and Certification	21
4. References	22

BLOOMBASE CONFIDENTIAL

BLOOMBASE CONFIDENTIAL

1. Document Revision History

Revision	Date	Revised By	Comments
0.9	2018-05-08	Michael Brew, Bloombase	Initial Draft for Discussion
0.91	2018-05-16	Michael Brew, Bloombase	Diagrams revised

BLOOMBASE CONFIDENTIAL

2. Introduction

This document outlines the use case scenarios of implementing Bloombase Next-Generation Data-at-Rest Encryption solution with VMware Cloud on Amazon Web Services (VMC on AWS).

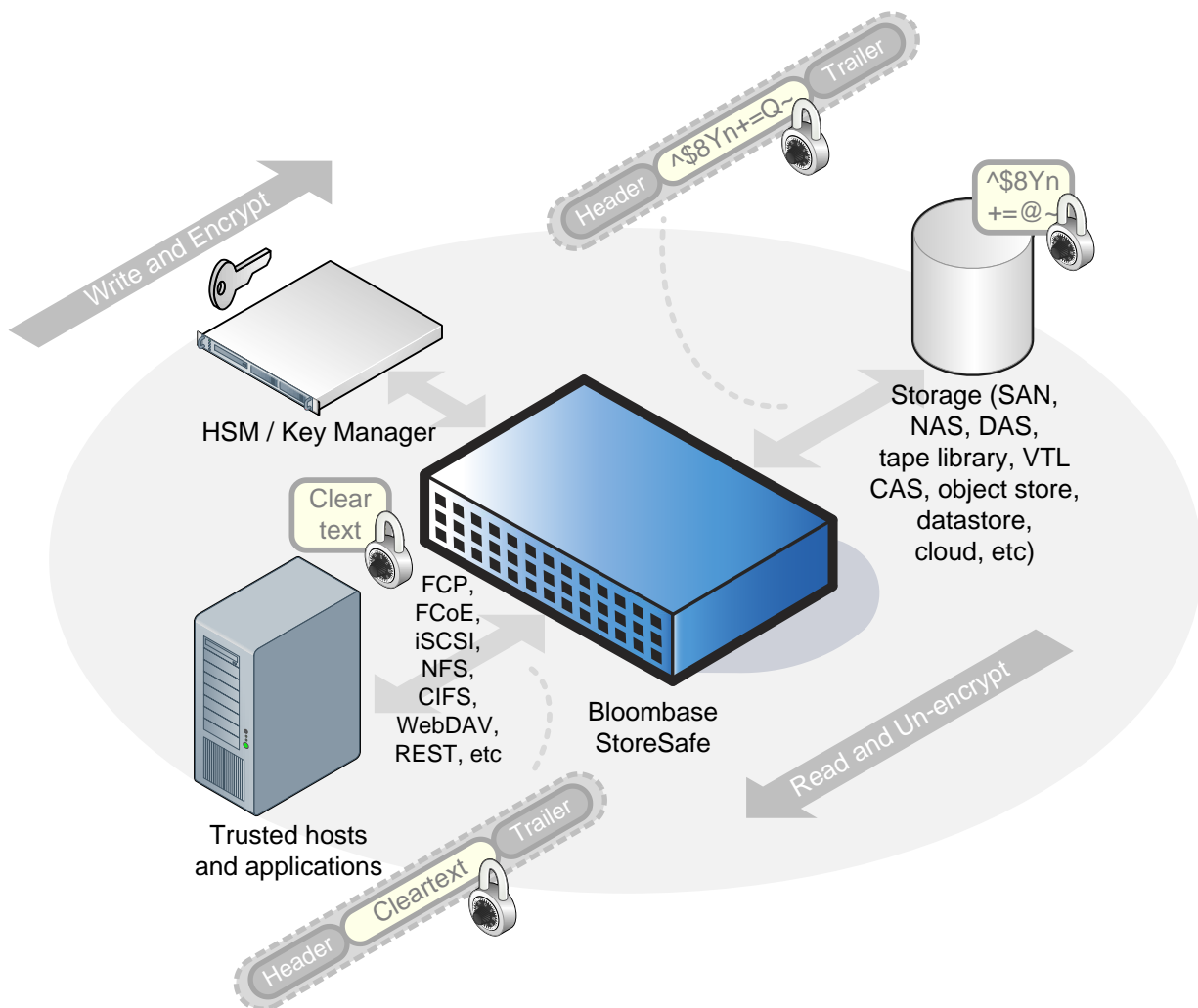
Traditional IT security measures regard outsiders as origins of cyber-attacks. Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), content filters, anti-virus, anti-malware, anti-spyware, SSL-VPN, Unified Threat Management (UTM), etc. all sits at the frontline defending core IT infrastructure at the perimeter only.

As unknown attacks, insider threats and targeted attacks are on the rise, sensitive and invaluable business data residing on core enterprise storage sub-systems in plain leaves business automation in huge vulnerabilities. Encryption of data-at-rest is generally perceived as the last-line-of-defense as inked in numerous industry best practices. Nevertheless, enterprises adopting application-specific encryption usually have to pay tremendous efforts on implementation and push the mission-critical applications in performance degradation and risks. The demand for application transparent data at-rest encryption solution and the drive for various information regulatory compliance which has to be high performance, easy to deploy, effortless integration, extensive infrastructure support, sustainable, scalable and fast to deploy as a turnkey solution drives the creation of Bloombase. Bloombase was created with the mission

BLOOMBASE CONFIDENTIAL

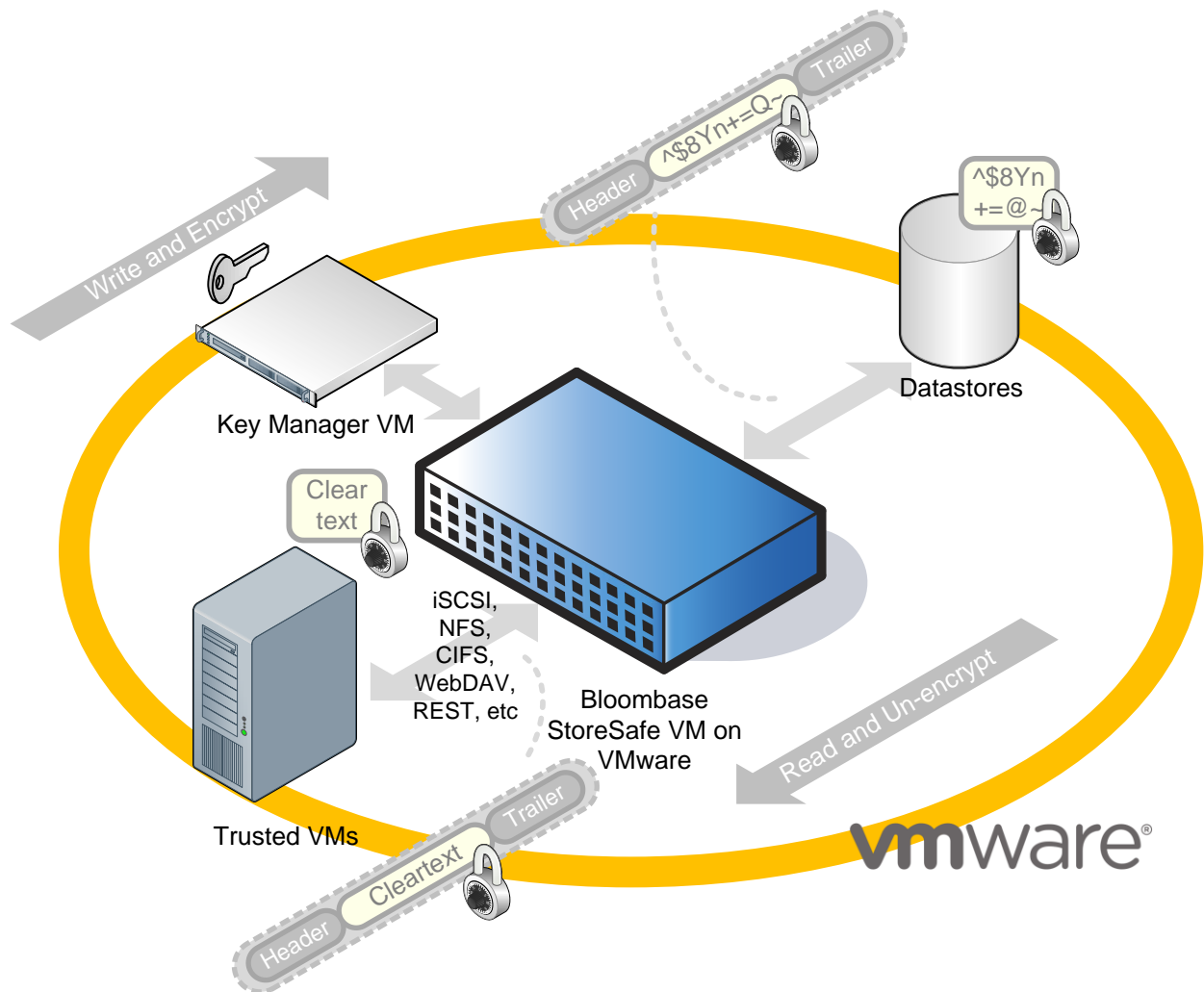
to address data security needs for both traditional IT and next-generation data-center infrastructures. Bloombase's goal to shrink-wrap the clear-text enterprise sensitive data-at-rest into cipher-text and enable trusted software applications and hosts to access the cipher-text data as-if they are in the clear.

Essentially Bloombase StoreSafe agentless unified storage encryption security solution performs as storage proxy running as bump-in-the-wire configuration providing transparent encryption and un-encryption of contents stored in enterprise Network Attached Storage (NAS), Storage Area Network (SAN), RESTful object stores, cloud storage service endpoints for authorized hosts and applications.



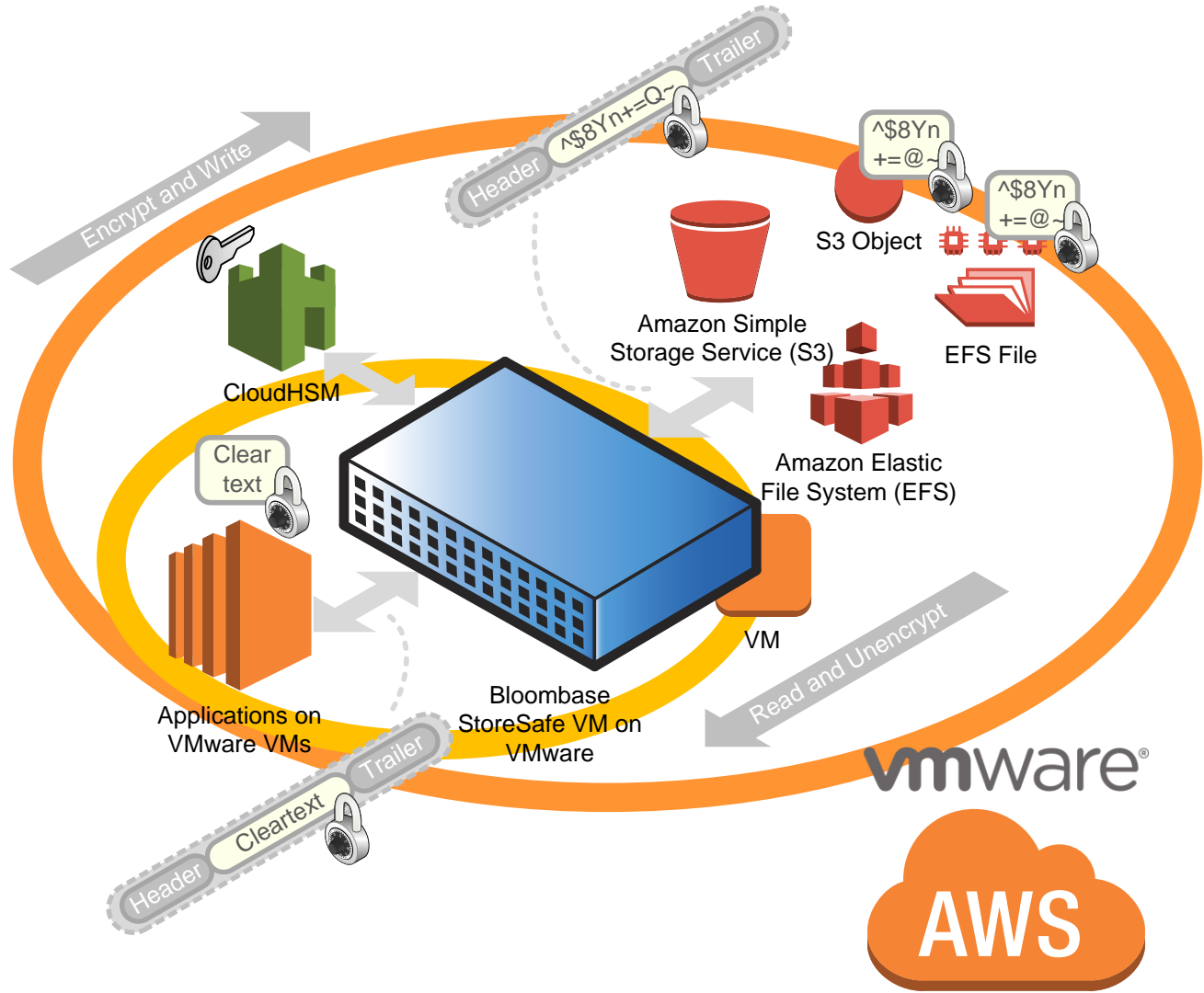
BLOOMBASE CONFIDENTIAL

Unlike traditional data at-rest encryption offerings in the market which form factor as proprietary hardware appliances, Bloombase assumes a transformative approach to provide real-time encryption of enterprise storage systems by a software-defined approach. Bloombase StoreSafe software appliance is ready to deploy on any x86-architecture hardware server appliance. Extending to the virtual data-center space, Bloombase StoreSafe offers the capability to run as virtual appliance on any QEMU-compliant virtual hypervisors securing virtual machine data and virtual storage systems. Bloombase also enables organizational customers to run Bloombase StoreSafe encryption as compute instance so as to scale encryption to data on the cloud and extend the capability to secure application workload on the cloud.



BLOOMBASE CONFIDENTIAL

This document outlines the use cases of Bloombase next-generation data encryption solution with VMware Cloud on Amazon Web Services (VMC on AWS) for mission-critical data-at-rest encryption protection for usage scenarios of encryption of Amazon Elastic File System (EFS) and Amazon Simple Storage Service (S3) with centralized Amazon CloudHSM key management.

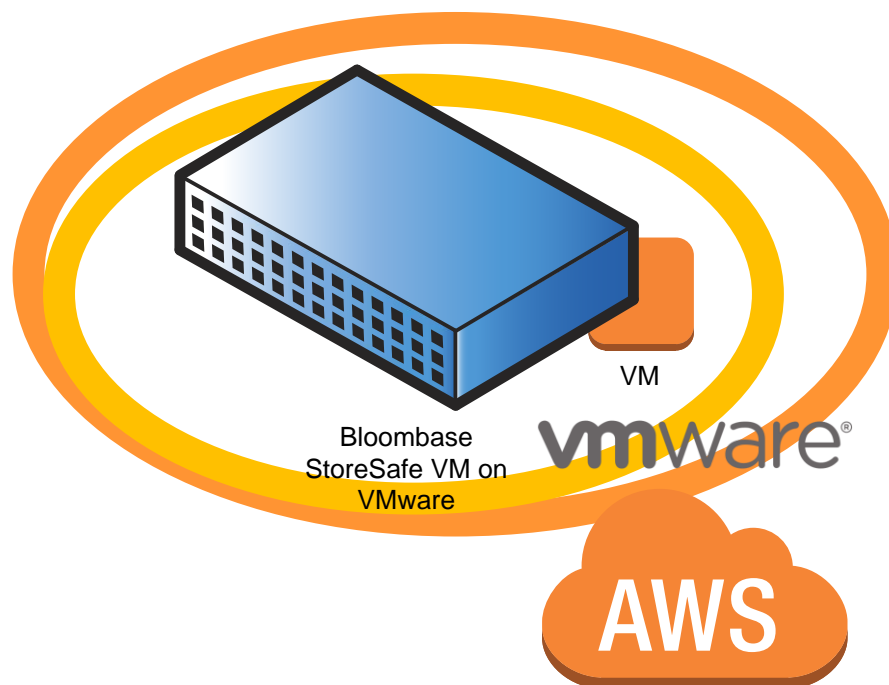


The following use cases cover all security capabilities supported by the Bloombase data-at-rest security solution.

BLOOMBASE CONFIDENTIAL

2.1 Use Cases for VMware Cloud on AWS

This section includes use cases of Bloomberg StoreSafe Virtual Appliance on VMC on AWS delivering security services as a VMware Virtual Machine.



2.1.1 Bloomberg StoreSafe deployment by OVF

Bloomberg StoreSafe OVF template created at on-premises VMware ESXi is deployed to the VMC on AWS for normal operation.

Example Use Case: Upload Bloomberg StoreSafe OVF template via the VMC web management console. A new Bloomberg StoreSafe virtual machine/appliance is deployed to VMC on AWS. The Bloomberg StoreSafe virtual machine is powered on to start delivering encryption services.

BLOOMBASE CONFIDENTIAL**2.1.2 Bloomberg StoreSafe deployment by vMotion**

Bloomberg StoreSafe virtual machine/appliance running on-premises VMware ESXi is migrated to the VMC on AWS using vMotion for normal operation.

Example Use Case: Migrate a Bloomberg StoreSafe virtual machine running on-premises to VMC on AWS via vMotion to deliver encryption services.

2.1.3 Bloomberg StoreSafe text console

Manage the Bloomberg StoreSafe virtual machine deployed on the VMC on AWS by accessing the text console.

Example Use Case: Access the Bloomberg StoreSafe text console at VMC console. Login with the same administrator credentials as the Bloomberg StoreSafe instance on-premises. Configure network parameters and bring the Bloomberg StoreSafe virtual machine online.

2.1.4 Bloomberg StoreSafe web management console

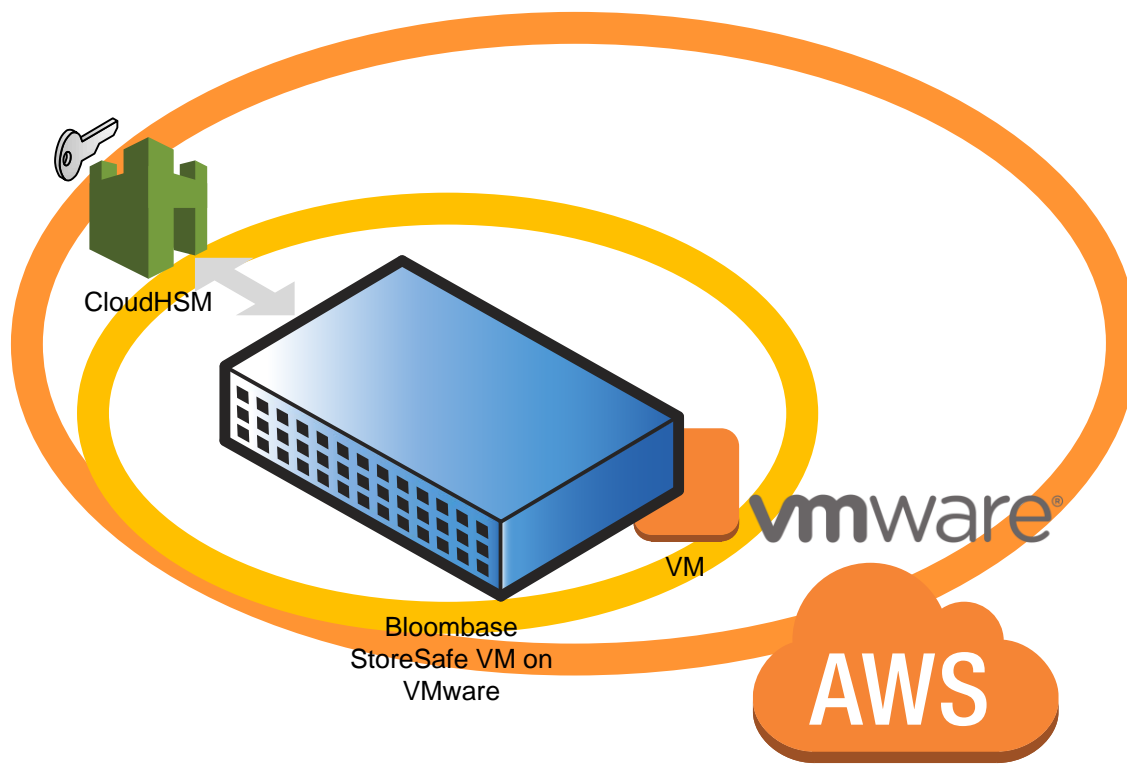
Manage the Bloomberg StoreSafe virtual machine deployed on the VMC on AWS by accessing the web management console.

Example Use Case: Access the Bloomberg StoreSafe web management URL at <https://<bloomberg>:8443> from a web browser. Login with the same administrator credentials as the Bloomberg StoreSafe instance on-premises. View dashboard.

2.2 Use Cases for Amazon CloudHSM

This section includes the use cases of Bloomberg StoreSafe Virtual Appliance on VMC on AWS delivering encryption security of data-at-rest with centralized key management at Amazon CloudHSM over PKCS#11 protocol.

BLOOMBASE CONFIDENTIAL



2.2.1 Bloomberg StoreSafe integration with Amazon CloudHSM for centralized lifecycle key management

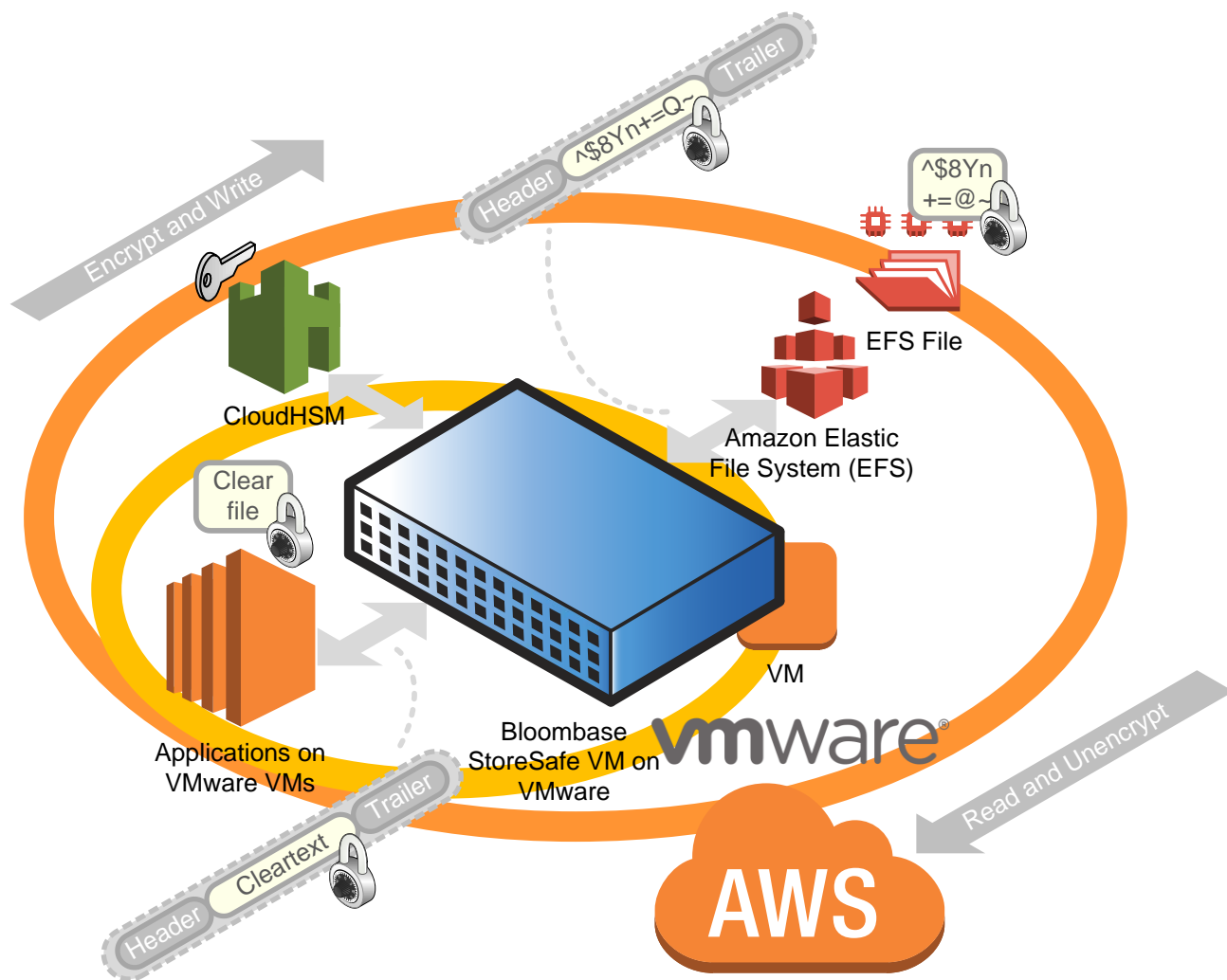
Bloomberg StoreSafe virtual machine when after migrated to VMC on AWS is able to access the pre-configured Amazon CloudHSM cryptographic key objects for data encryption security processing.

Example Use Case: Access Bloomberg StoreSafe web management console to inquire and test connectivity to the cryptographic key objects managed at Amazon CloudHSM.

2.3 Use Cases for Amazon Elastic File System (EFS)

This section includes the use cases of Bloomberg StoreSafe Virtual Appliance on VMC on AWS delivering encryption security of Amazon Elastic File System (EFS) as storage backend over NFS network storage protocol.

BLOOMBASE CONFIDENTIAL



2.3.1 Bloombase StoreSafe NFS virtual storage with host network access control

Only authorized hosts are allowed to access Bloombase StoreSafe NFS virtual storages.

Example Use Case: Access Bloombase StoreSafe NFS virtual storage at host with authorized IP network address resulting in successful connection to Bloombase StoreSafe NFS virtual storage, otherwise, access denied error is returned.

BLOOMBASE CONFIDENTIAL**2.3.2 Bloomberg StoreSafe NFS virtual storage**

List and browse Bloomberg StoreSafe NFS virtual storages.

Example Use Case: List and browse Bloomberg StoreSafe NFS virtual storages from host with authorized IP network address resulting in listing of Bloomberg StoreSafe NFS virtual storage network shares.

2.3.3 Bloomberg StoreSafe NFS virtual storage network share connection

Connect and access Bloomberg StoreSafe NFS virtual storages.

Example Use Case: Access Bloomberg StoreSafe NFS virtual storage from host with authorized IP network address resulting in successful connection to Bloomberg StoreSafe NFS virtual storage network shares, otherwise, access denied error is returned.

2.3.4 Mount Bloomberg StoreSafe NFS virtual storage

Mount Bloomberg StoreSafe NFS virtual storage as network mount-point.

Example Use Case: Mount Bloomberg StoreSafe NFS virtual storage from host with authorized IP network address resulting in successful connection to Bloomberg StoreSafe NFS virtual storage and be able to access as a network mount-point on Linux.

2.3.5 Store and encrypt contents at Bloomberg StoreSafe NFS virtual storage via mount point

Store files at Bloomberg StoreSafe NFS virtual storage as network drive with contents encrypted and persisted physically at backend Amazon EFS.

Example Use Case: Create and store files or folders at mounted Bloomberg StoreSafe NFS virtual storage from host with authorized IP network address as network mount-point as if normal virtual-plain files and folders. Search for known-text contents at physical Amazon EFS as NFS network share resulting not found as entire contents of file are fully encrypted by Bloomberg StoreSafe.

BLOOMBASE CONFIDENTIAL**2.3.6 Retrieve and un-encrypt contents at Bloomberg StoreSafe NFS virtual storage via local file system**

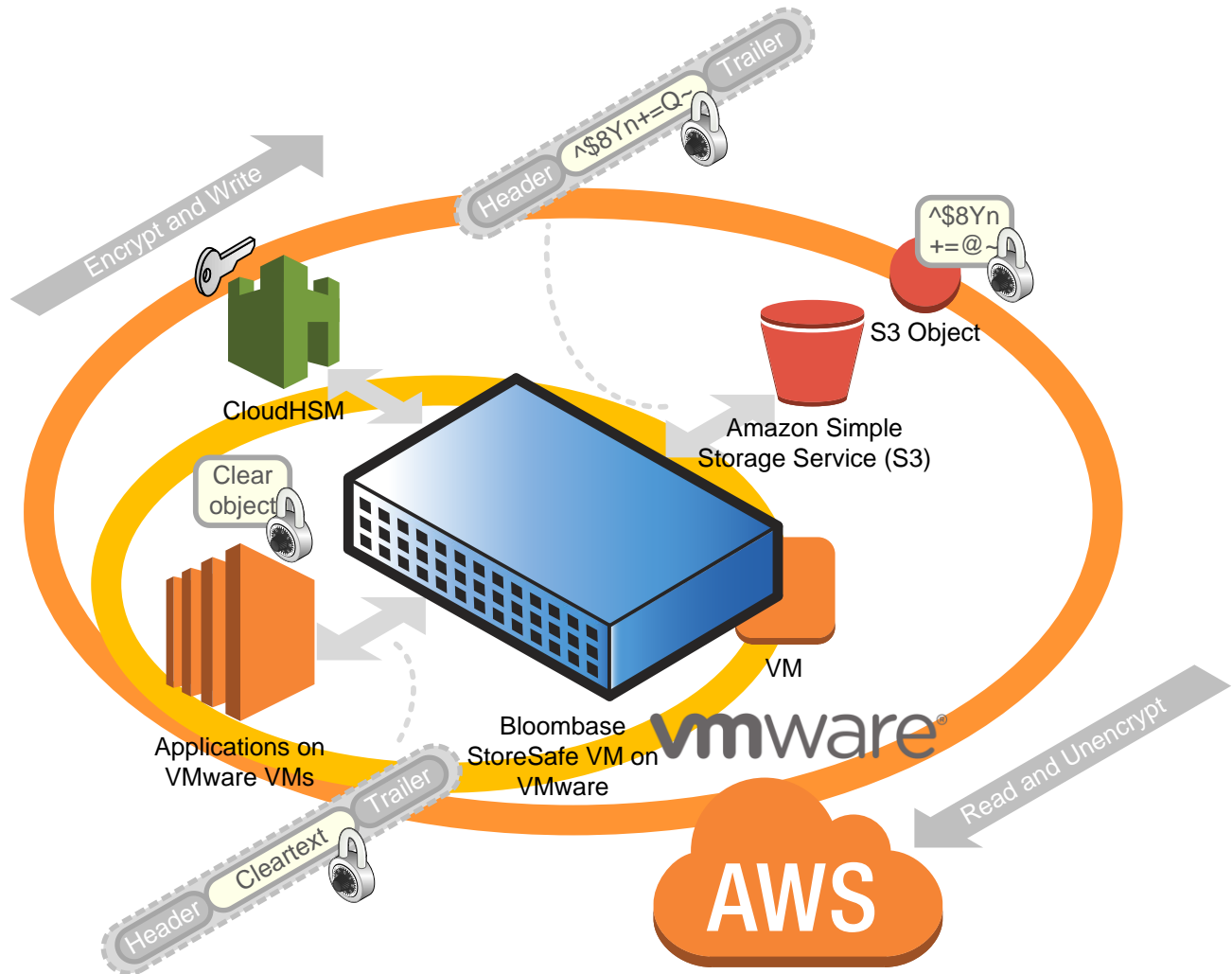
Retrieve files and contents at Bloomberg StoreSafe NFS virtual storage as network drive with contents un-encrypted as retrieved from backend Amazon EFS.

Example Use Case: Access and read files or folders at mounted Bloomberg StoreSafe NFS virtual storage from host with authorized IP network address as network mount-point as if normal virtual-plain files and folders.

2.4 Use Cases for Amazon Simple Storage Service (S3)

This section includes use cases of Bloomberg StoreSafe Virtual Appliance on VMC on AWS delivering encryption security of Amazon Simple Storage Service (S3) as storage backend over REST/HTTP network storage protocol.

BLOOMBASE CONFIDENTIAL



2.4.1 Bloombase StoreSafe S3 virtual storage with access control

Only authorized clients are allowed to access Bloombase StoreSafe S3 virtual storages.

Example Use Case: Access Bloombase StoreSafe S3 virtual storage at host with authorized credentials resulting in successful connection to Bloombase StoreSafe S3 virtual storage, otherwise, access denied error is returned.

BLOOMBASE CONFIDENTIAL**2.4.2 Bloomberg StoreSafe S3 virtual storage**

List and browse Bloomberg StoreSafe S3 virtual storages as S3 buckets.

Example Use Case: List and browse Bloomberg StoreSafe S3 virtual storages from host with authorized credentials resulting in listing of Bloomberg StoreSafe S3 virtual storage in form of S3 buckets.

2.4.3 Bloomberg StoreSafe S3 virtual storage network share connection

Connect and access Bloomberg StoreSafe S3 virtual storages.

Example Use Case: Access Bloomberg StoreSafe S3 virtual storage from host with authorized credentials resulting in successful connection to Bloomberg StoreSafe S3 virtual storage as S3 buckets, otherwise, access denied error is returned.

2.4.4 Store and encrypt contents at Bloomberg StoreSafe S3 virtual storage

Store objects at Bloomberg StoreSafe S3 virtual storage as generic S3 bucket with contents encrypted and persisted physically at backend Amazon S3 bucket.

Example Use Case: Create and store objects at Bloomberg StoreSafe S3 virtual storage from host with authorized credentials as if normal virtual-plain objects. Retrieve physical object from backend Amazon S3 to examine if contents are in cipher-text form.

2.4.5 Retrieve and un-encrypt contents at Bloomberg StoreSafe S3 virtual storage

Retrieve objects at Bloomberg StoreSafe S3 virtual storage as generic S3 bucket with contents un-encrypted as retrieved from backend Amazon S3 bucket.

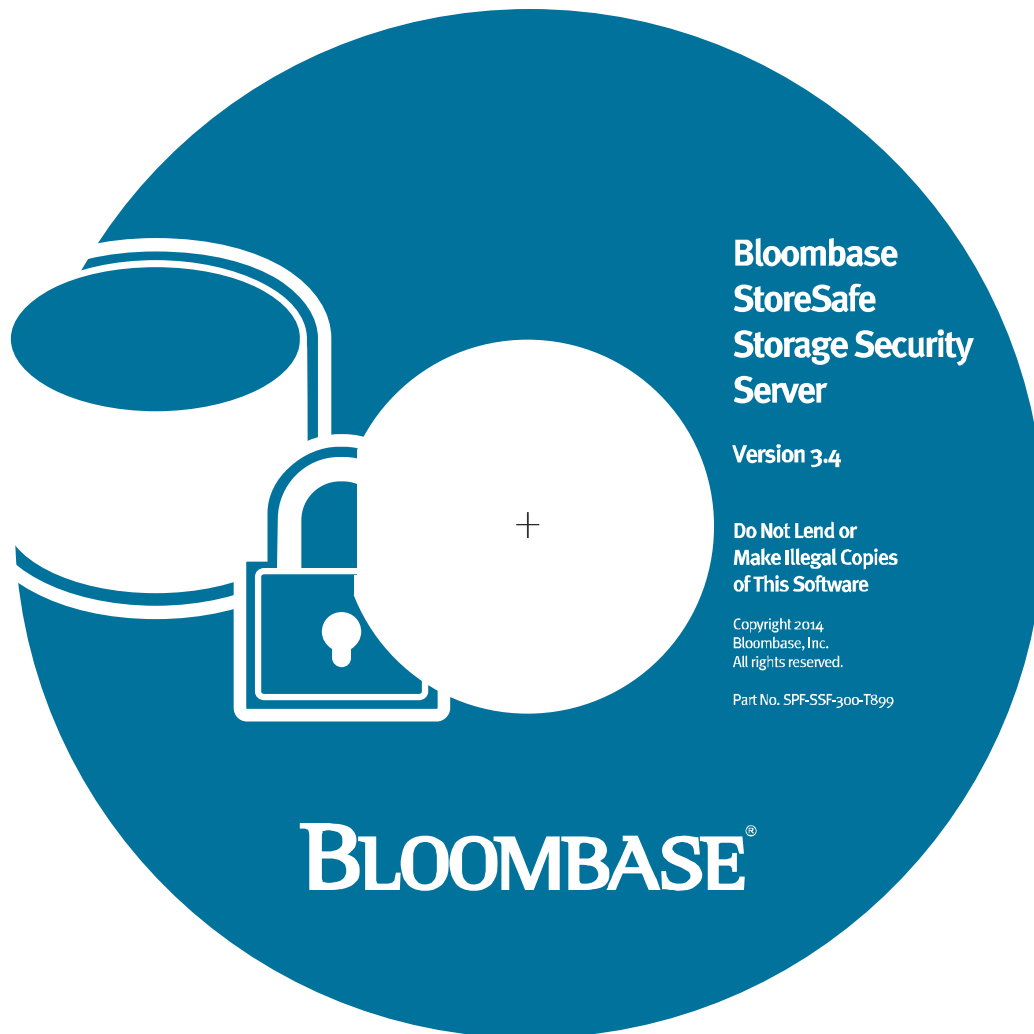
Example Use Case: Access and read objects at Bloomberg StoreSafe S3 virtual storage from host with authorized credentials as if normal virtual-plain objects.

BLOOMBASE CONFIDENTIAL

2.5 The Bloomberg Solution Configuration Screens

2.5.1 Installation

The Bloomberg StoreSafe software appliance in form of ISO images can be directly mounted as virtual disk media on VMware ESXi for virtual appliance installation or are available as installation CD/DVD to be installed directly from disk drives for hardware appliance deployment.



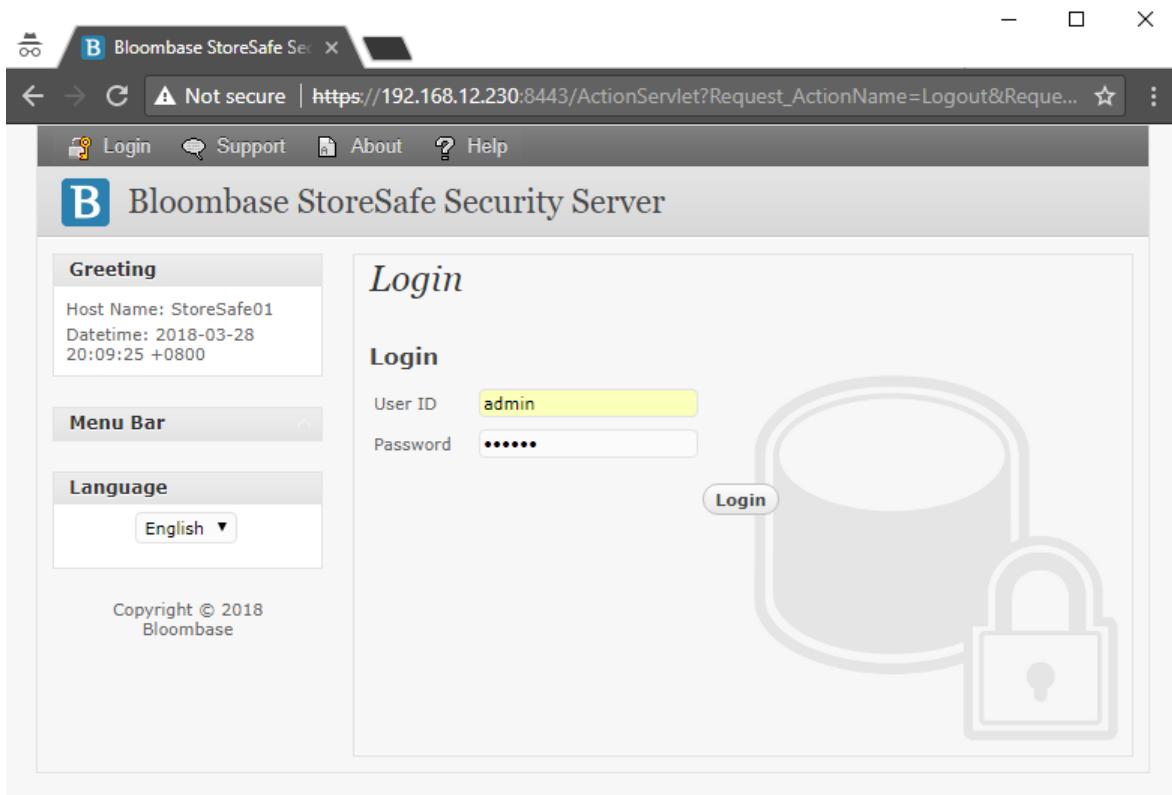
Bloomberg StoreSafe can also be deployed on VMware ESXi as OVF template or by utilizing vMotion tool.

Bloomberg StoreSafe software appliance installer will guide you through the rest of the installation process.

BLOOMBASE CONFIDENTIAL

2.5.2 Management

Bloombase StoreSafe Web Administration Console Login page.



The Main dashboard page of the Bloombase StoreSafe web console displays the system and server information.

BLOOMBASE CONFIDENTIAL

Bloombase StoreSafe Security Server

Host Name: StoreSafe01
User: admin
Datetime: 2018-03-28 20:11:34 +0800

Menu Bar

- System
- Operation
- Network Security
- High Availability
- Administration
- Key Management
- StoreSafe Configurations
- Storage

Language: English

Copyright © 2018 Bloombase

Main

System Information

Product Name	Bloombase StoreSafe Security Server	Version	3.4.6.21
Host Name	StoreSafe01 / localhost	System Up Since	2018-03-24 01:55:10 +0800
Host Addresses	1 ens192 fe80:0:0:0:250:56ff:fe87:66c6, 192.168.12.230		
Licensee	C=US O=Bloombase\ Inc. CN=SPFSSF2666	Serial Number	9830
Validity	<input checked="" type="checkbox"/>	Perpetuality	<input checked="" type="checkbox"/>

Server Information

Operating System	Linux amd64 3.10.0-327.el7.ssfc.x86_64	Processors	1
Memory Utilization	3%	Total Memory	519,110,656
Max Memory	4,151,836,672	Free Memory	380,883,064
Disk Space Utilization	25%	Total Disk Space	14,879,293,440
Used Disk Space	3,739,713,536	Free Disk Space	11,139,579,904

Application Status

Application Status:

Last Shutdown Time
Last Standby Time
Last Startup Time: 2018-03-24 01:55:18 +0800

BLOOMBASE CONFIDENTIAL

3. Bloombase Interoperability and Certification

Certification of Bloombase StoreSafe with VMware Cloud on Amazon Web Services (VMC on AWS) will be deemed complete and accepted by Bloombase when the Use Case designs in this document are demonstrated on a releasable version of the VMware Cloud on AWS.

An Exit Form document for each platform will be co-developed to capture the detailed test scenarios for Certification.

BLOOMBASE CONFIDENTIAL

4. References

Bloombase StoreSafe, <https://www.bloombase.com/products/storesafe/>

VMware Cloud on AWS, <https://cloud.vmware.com/vmc-aws>

AWS CloudHSM, <https://aws.amazon.com/cloudhsm>

Amazon Elastic File System (EFS), <https://aws.amazon.com/efs>

Amazon Simple Storage Service (S3), <https://aws.amazon.com/s3>