High Level Integration Document

Current Version	**1.0**
Approved By	
Approval Date	

Dell EqualLogic and Compellent Platform – Use Cases & Certification: Bloombase - Phase 1 (UCC)

Table of Contents

1 Document Revision History

Revision	Date	Revised By	Comments
0.1	05/11/2012	Dell	Initial Draft For Discussion
0.2	06/01/2012	Bloombase	Template details for Bloombase applications
1.0	07/09/2012	Dell	Final Update

2 Introduction

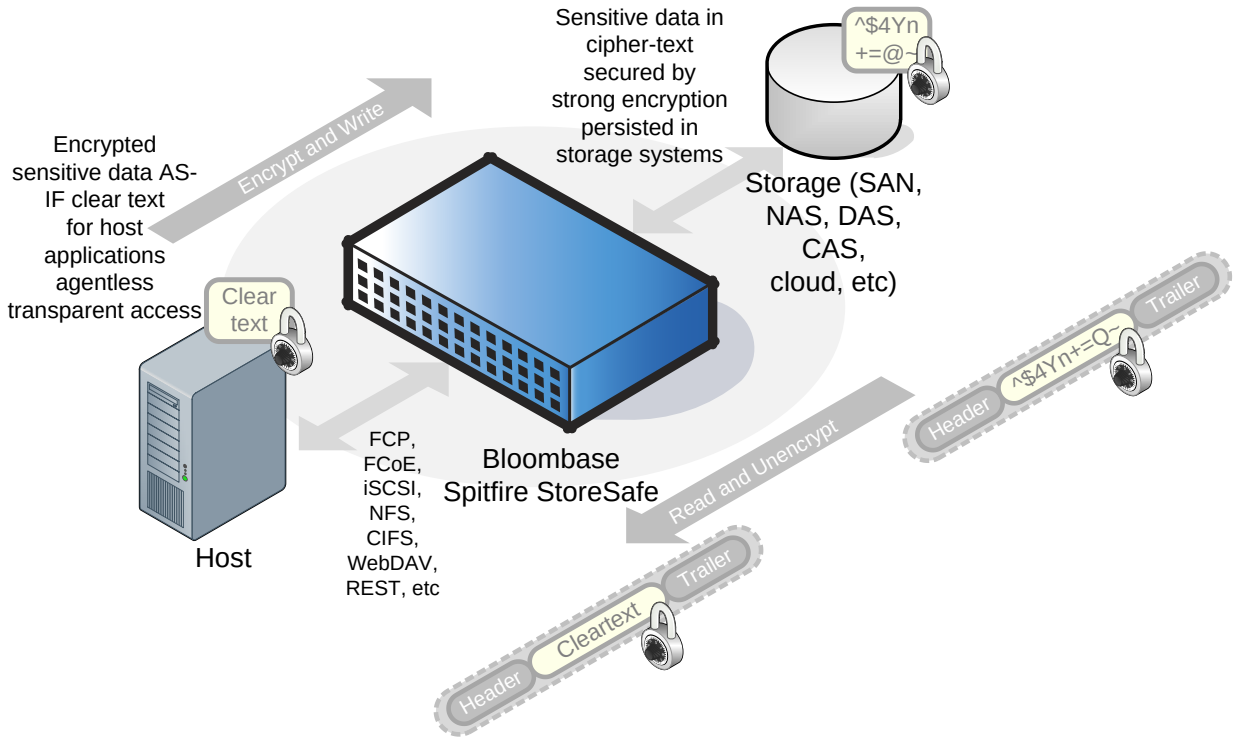
This document outlines the use case scenarios of implementing Bloombase Non-Disruptive Transparent Storage Encryption solution on Dell PowerEdge server and Dell Storage Devices including Equallogic and Compellent system.

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 at-rest data 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 deployment as a turnkey solution drives the creation of Bloombase.

Bloombase was created with the mission to address Unified Critical Data Protection (UCDP). Bloombase's goal to put clothes on the naked enterprise critical at-rest data and enable data owners to change easily and securely.

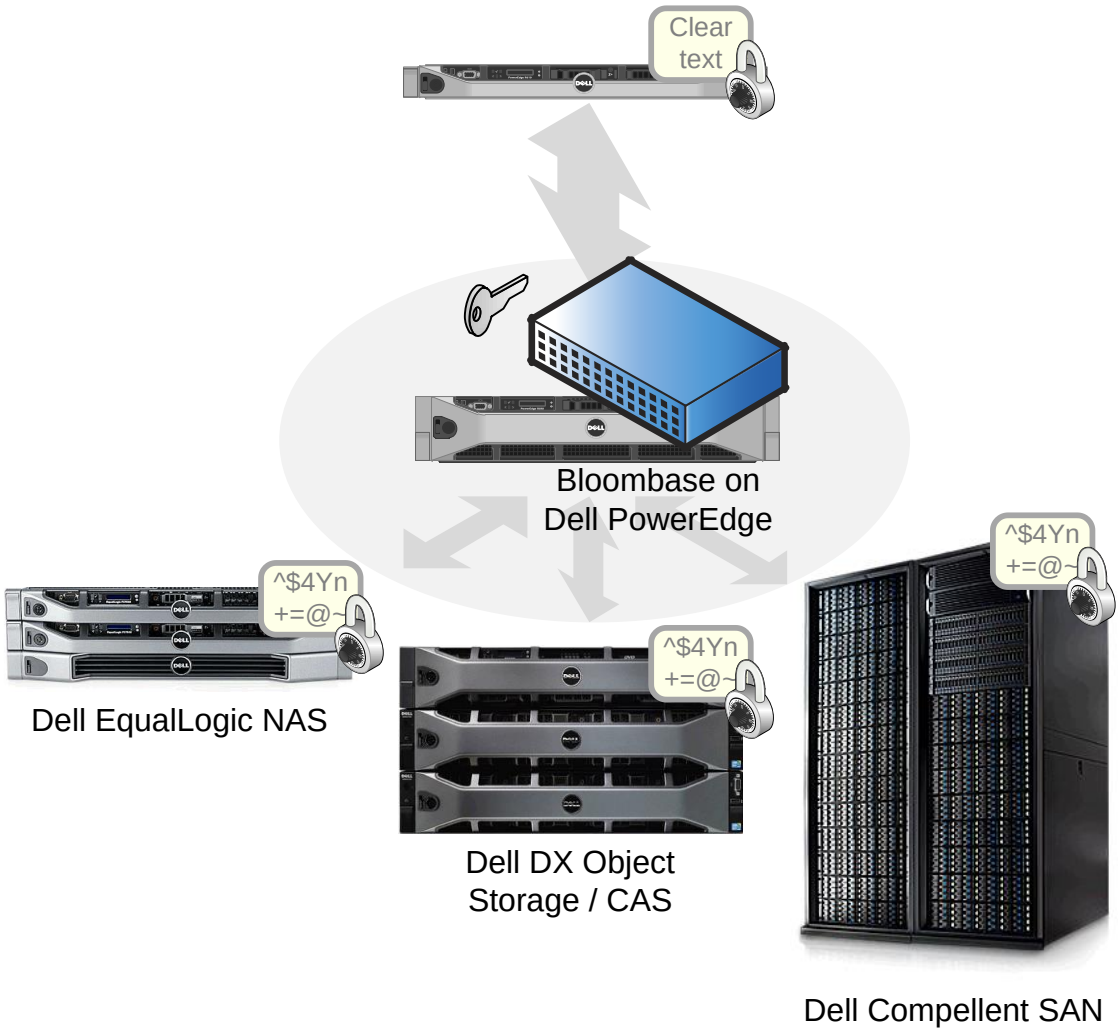
Essentially Bloombase Spitfire StoreSafe agentless unified storage encryption security solution performs as storage proxy running as a bump-in-the-wire configuration providing transparent encryption and un-encryption of contents stored in enterprise Network Attached Storage (NAS), Storage Area Network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



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-only implementation. Bloombase Spitfire StoreSafe is ready to deploy on any x86-architecture hardware server appliance. Extending to the virtual data center space, Bloombase Spitfire StoreSafe offers the capability to run as virtual appliance on any QEMU-compliant virtual hypervisors securing virtual machine data and virtual storage systems.

Dell offers a complete hardware solution from server computing, network connectivity, storage connectivity, object, file, and block storage infrastructure powering mission critical applications for enterprises of all sizes.

Enter Bloombase data at-rest security software solution, not only Dell provides the high performance and highly scalable compute node PowerEdge servers which Bloombase Spitfire StoreSafe encryption software runs on, Dell also houses business critical information on their Compellent, Equallogic and DX object store in which business secrets and sensitive data are kept away from unauthorized access by Bloombase encryption.

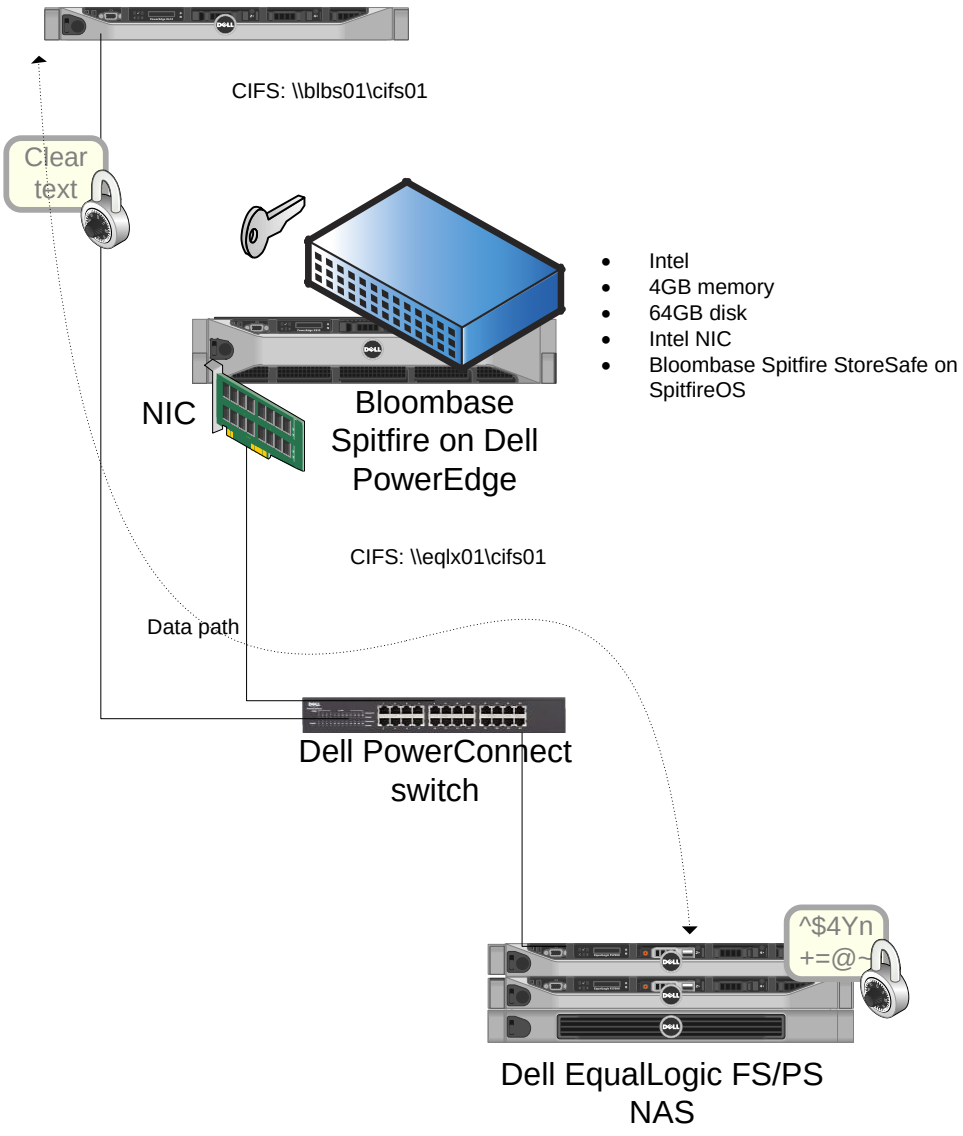


The following use cases will cover all encryption capabilities achieved by the Bloombase solution.

2.1 Use Cases for Equallogic as the storage device for CIFS security

The Use Cases for supporting Equallogic as the storage system for CIFS security with PowerEdge server for Bloombase solution.

- NIC
- Microsoft Windows Server 2008



2.1.1 CIFS user authentication access control

User authentication at Windows Server 2008 by Bloombase Spitfire StoreSafe CIFS virtual storage will be supported.

Example Use Case: Access Bloombase Spitfire StoreSafe CIFS virtual storage at Windows Server 2008 Windows Explorer \\blbs01\cifs01 where correct user name and password combination yields successful user authentication access control at Bloombase Spitfire StoreSafe before the CIFS virtual storage is connected. Incorrect user name and password combination should yield request for retry.

2.1.2 Host network access control

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

Example Use Case: Access Bloombase Spitfire StoreSafe CIFS virtual storage at Windows Server 2008 Windows Explorer \\blbs01\cifs01 with authorized IP network address with correct user authentication credentials yields successful connection to Bloombase Spitfire StoreSafe CIFS virtual storage. Otherwise, access denied.

2.1.3 Connect to Bloombase Spitfire CIFS virtual storages

Connection established for Windows Server 2008 user session to Bloombase Spitfire StoreSafe CIFS virtual storage and host applications be able to connect and access as if normal CIFS network shares.

Example Use Case: User presents correct combination of username and password at authorized Windows Server 2008 host successfully connects to Bloombase Spitfire StoreSafe CIFS virtual storage \\blbs01\cifs01 at Windows Explorer

2.1.4 List of Bloombase Spitfire CIFS virtual storages

Connected Bloombase Spitfire StoreSafe CIFS virtual storage contents listable.

Example Use Case: On successful user and host access control at Windows Server 2008 by Bloombase Spitfire StoreSafe CIFS virtual storage at \\blbs01\cifs01, user should be able to list files and folders at Windows Explorer.

2.1.5 Write and encrypt files to Bloombase Spitfire CIFS virtual storages

Create or copy files to Bloombase Spitfire CIFS virtual storages and contents get encrypted

Example Use Case: On successful user and host access control at Windows Server 2008 by Bloombase Spitfire StoreSafe CIFS virtual storage at \\blbs01\cifs01, user creates or copy files to base or subfolders of Bloombase Spitfire CIFS virtual storage successfully. Examine contents of same file at \\eqlx01\cifs01 for ciphertext.

2.1.6 Read and un-encrypt files from Bloombase Spitfire CIFS virtual storages

Access and open encrypted files at Bloombase Spitfire StoreSafe CIFS virtual storages and obtain virtual-plain contents

Example Use Case: On successful user and host access control at Windows Server 2008 by Bloombase Spitfire StoreSafe CIFS virtual storage at \\blbs01\cifs01, user opens and read virtual-plain text of encrypted files physically stored at Dell Equallogic \\eqlx01\cifs01 via Bloombase Spitfire StoreSafe.

2.1.7 Update files from Bloombase Spitfire CIFS virtual storages

Update contents of encrypted files at Bloombase Spitfire StoreSafe CIFS virtual storages as-if virtual-plain contents

Example Use Case: On successful user and host access control at Windows Server 2008 by Bloombase Spitfire StoreSafe CIFS virtual storage at \\blbs01\cifs01, user opens encrypted files at \\eqlx01\cifs01 via Bloombase Spitfire StoreSafe as-if virtual plain contents, alters or updates contents in file and save to Dell Equallogic via Bloombase Spitfire StoreSafe CIFS virtual storage yields automatic encryption.

2.1.8 Delete files from Bloombase Spitfire CIFS virtual storages

Delete files from Bloombase Spitfire StoreSafe CIFS virtual storages as-if normal files

Example Use Case: On successful user and host access control at Windows Server 2008 by Bloombase Spitfire StoreSafe CIFS virtual storage at \\blbs01\cifs01, user deletes a file via Bloombase Spitfire StoreSafe where the actual file storing contents as encrypted at Equallogic gets deleted also

2.1.9 Create folders in Bloombase Spitfire CIFS virtual storages

Create folders from Bloombase Spitfire StoreSafe CIFS virtual storages as normal folders

Example Use Case: On successful user and host access control at Windows Server 2008 by Bloombase Spitfire StoreSafe CIFS virtual storage at \\blbs01\cifs01, user creates a folder via Bloombase Spitfire StoreSafe using Windows Explorer and same folder is created at Dell

Equallogic \\eqlx01\cifs01.

2.1.10 Open folder in Bloombase Spitfire CIFS virtual storages

Access and open folders at Bloombase Spitfire StoreSafe CIFS virtual storages as normal folders.

Example Use Case: On successful user and host access control at Windows Server 2008 by Bloombase Spitfire StoreSafe CIFS virtual storage at \\blbs01\cifs01, user opens folders under Bloombase Spitfire StoreSafe CIFS virtual storages via Windows Explorer.

2.1.11 Delete folders in Bloombase Spitfire CIFS virtual storages

Delete folders at Bloombase Spitfire StoreSafe CIFS virtual storages

Example Use Case: On successful user and host access control at Windows Server 2008 by Bloombase Spitfire StoreSafe CIFS virtual storage at \\blbs01\cifs01, user deletes folders under Bloombase Spitfire StoreSafe CIFS virtual storages via Windows Explorer and yield the actual folder stored at Dell Equallogic \\eqlx01\cifs01 gets actually deleted.

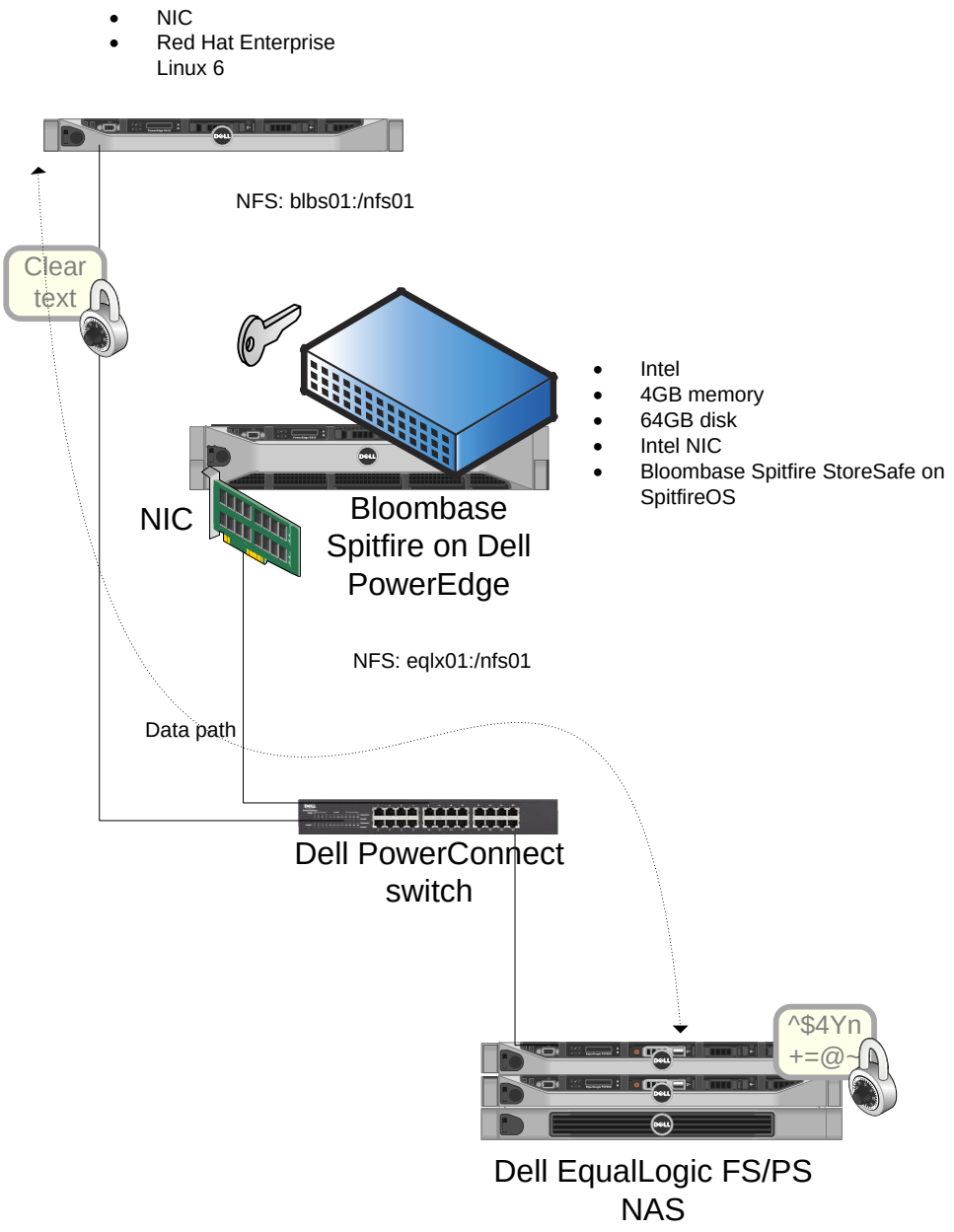
2.1.12 Write-once-read-many (WORM) in Bloombase Spitfire CIFS virtual storages

Bloombase Spitfire StoreSafe CIFS virtual storages behave as a logic write-once-read-many (WORM) for secure archival use

Example Use Case: On successful user and host access control at Windows Server 2008 by Bloombase Spitfire StoreSafe CIFS virtual storage at \\blbs01\cifs01, user copies or moves files to Bloombase Spitfire StoreSafe CIFS WORM virtual storages and gets actually persisted at Dell Equallogic at \\eqlx01\cifs01, such file(s) are read-only blocking rewrite of such files via Bloombase Spitfire StoreSafe CIFS virtual storages for long term secure retention. If hackers or crackers alter contents at Equallogic, the files rendered via Bloombase Spitfire StoreSafe as tampered and corrupted yielding I/O errors as proof of tampering.

2.2 Use Cases for Equallogic as the storage device for NFS security

The Use Cases for supporting Equallogic as the storage system for NFS security with PowerEdge server for Bloombase solution.



2.2.1 Host network access control

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

Example Use Case: Access Bloombase Spitfire StoreSafe CIFS virtual storage at Red Hat Enterprise Linux command prompt blbs01:/nfs01 with authorized IP network address yields successful connection to Bloombase Spitfire StoreSafe NFS virtual storage. Otherwise, access denied.

2.2.2 Connect to Bloombase Spitfire NFS virtual storages

Connection established for Red Hat Enterprise Linux to Bloombase Spitfire StoreSafe NFS virtual storage and host applications be able to connect and access as if normal NFS network shares and mount points.

Example Use Case: Administrator mounts at authorized Linux successfully connects to Bloombase Spitfire StoreSafe NFS virtual storage blbs01:/nfs01 at command prompt.

2.2.3 List of Bloombase Spitfire NFS virtual storages

Connected Bloombase Spitfire StoreSafe NFS virtual storage contents listable.

Example Use Case: On successful host access control at Red Hat Enterprise Linux Server by Bloombase Spitfire StoreSafe NFS virtual storage at blbs01:/nfs01, administrator should be able to list files and folders using ls command.

2.2.4 Write and encrypt files to Bloombase Spitfire NFS virtual storages

Create or copy files to Bloombase Spitfire NFS virtual storages and contents get encrypted

Example Use Case: On successful host access control at Red Hat Enterprise Linux Server by Bloombase Spitfire StoreSafe NFS virtual storage at blbs01:/nfs01, administrator creates or copy files to base or subfolders of Bloombase Spitfire NFS virtual storage successfully. Examine contents of same file at eqlx01:/nfs01 for ciphertext.

2.2.5 Read and un-encrypt files from Bloombase Spitfire NFS virtual storages

Access and open encrypted files at Bloombase Spitfire StoreSafe NFS virtual storages and obtain virtual-plain contents

Example Use Case: On successful host access control at Red Hat Enterprise Linux Server by Bloombase Spitfire StoreSafe NFS virtual storage at blbs01:/nfs01, administrator opens and read virtual-plain text of encrypted files physically stored at Dell Equallogic eqlx01:/nfs01 via Bloombase Spitfire StoreSafe.

2.2.6 Update files from Bloombase Spitfire NFS virtual storages

Update contents of encrypted files at Bloombase Spitfire StoreSafe NFS virtual storages as-if virtual-plain contents

Example Use Case: On successful host access control at Red Hat Enterprise Linux Server by Bloombase Spitfire StoreSafe NFS virtual storage at blbs01:/nfs01, administrator opens encrypted files at eqlx01:/nfs01 via Bloombase Spitfire StoreSafe as-if virtual plain contents using vi, alters or updates contents in file and save to Dell Equallogic via Bloombase Spitfire StoreSafe NFS virtual storage yields automatic encryption.

2.2.7 Delete files from Bloombase Spitfire NFS virtual storages

Delete files from Bloombase Spitfire StoreSafe NFS virtual storages as-if normal files

Example Use Case: On successful host access control at Red Hat Enterprise Linux Server by Bloombase Spitfire StoreSafe NFS virtual storage at blbs01:/nfs01, administrator deletes a file via Bloombase Spitfire StoreSafe where the actual file storing contents as encrypted at Equallogic gets deleted also using rm command.

2.2.8 Create folders in Bloombase Spitfire NFS virtual storages

Create folders from Bloombase Spitfire StoreSafe NFS virtual storages as normal folders

Example Use Case: On successful host access control at Red Hat Enterprise Linux Server by Bloombase Spitfire StoreSafe NFS virtual storage at blbs01:/nfs01, administrator creates a folder via Bloombase Spitfire StoreSafe at command prompt using mkdir command and same folder is created at Dell Equallogic eqlx01:/nfs01.

2.2.9 Open folder in Bloombase Spitfire NFS virtual storages

Access and open folders at Bloombase Spitfire StoreSafe NFS virtual storages as normal folders.

Example Use Case: On successful host access control at Red Hat Enterprise Linux Server by Bloombase Spitfire StoreSafe NFS virtual storage at blbs01:/nfs01,administrator opens folders under Bloombase Spitfire StoreSafe NFS virtual storages at command prompt using cd command.

2.2.10 Delete folders in Bloombase Spitfire CIFS virtual storages

Delete folders at Bloombase Spitfire StoreSafe NFS virtual storages

Example Use Case: On successful host access control at Red Hat Enterprise Linux Server by Bloombase Spitfire StoreSafe NFS virtual storage at blbs01:/nfs01, administrator deletes folders under Bloombase Spitfire StoreSafe NFS virtual storages at command prompt using rmdir command and yield the actual folder stored at Dell Equallogic eqlx01:/nfs01 gets actually deleted.

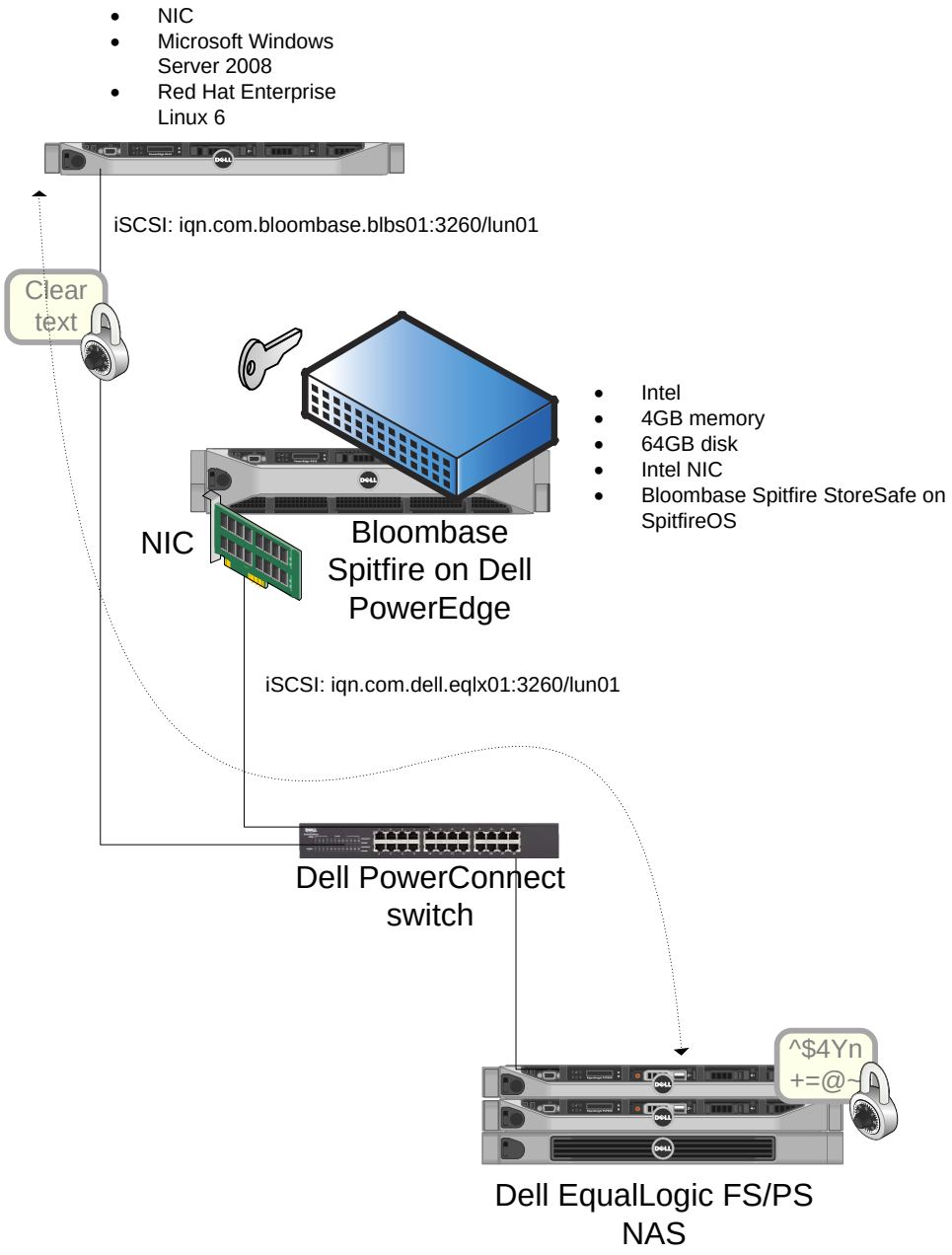
2.2.11 Write-once-read-many (WORM) in Bloombase Spitfire NFS virtual storages

Bloombase Spitfire StoreSafe NFS virtual storages behave as a logic write-once-read-many (WORM) for secure archival use

Example Use Case: On successful host access control at Red Hat Enterprise Linux Server by Bloombase Spitfire StoreSafe NFS virtual storage at blbs01:/nfs01, administrator copies or moves files to Bloombase Spitfire StoreSafe NFS WORM virtual storages and gets actually persisted at Dell Equallogic at eqlx01:/nfs01, such file(s) are read-only blocking rewrite of such files via Bloombase Spitfire StoreSafe NFS virtual storages for long term secure retention. If hackers or crackers alter contents at Equallogic, the files rendered via Bloombase Spitfire StoreSafe as tampered and corrupted yielding I/O errors as proof of tampering.

2.3 Use Cases for Equallogic as the storage device for iSCSI security

The Use Cases for supporting Equallogic as the storage system for iSCSI security with PowerEdge server for Bloombase solution.



2.3.1 Bloombase Spitfire StoreSafe iSCSI virtual storage CHAP user authentication access control

CHAP user authentication at Windows Server 2008 or Red Hat Enterprise Linux by Bloombase Spitfire StoreSafe iSCSI virtual storage will be supported.

Example Use Case: Discover and access Bloombase Spitfire StoreSafe iSCSI virtual storage at Windows Server 2008 or Linux using software initiator where correct CHAP user name and password combination yields successful user authentication access control at Bloombase Spitfire StoreSafe before the iSCSI virtual storage is connected. Incorrect user name and password combination should deny access.

2.3.2 Host network access control

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

Example Use Case: Access Bloombase Spitfire StoreSafe iSCSI virtual storage at Windows Server 2008 or Linux with authorized IP network address with correct CHAP user authentication credentials yields successful connection to Bloombase Spitfire StoreSafe iSCSI virtual storage. Otherwise, access denied.

2.3.3 Bloombase Spitfire StoreSafe iSCSI virtual storage target discovery

List and discover Bloombase Spitfire StoreSafe iSCSI virtual storages.

Example Use Case: Discover and list Bloombase Spitfire StoreSafe iSCSI virtual storages at Windows Server 2008 or Linux with authorized IP network address with correct CHAP user authentication credentials yields discovery and listing of Bloombase Spitfire StoreSafe iSCSI virtual storages.

2.3.4 Bloombase Spitfire StoreSafe iSCSI virtual storage target connection

Connect and access Bloombase Spitfire StoreSafe iSCSI virtual storages.

Example Use Case: Access Bloombase Spitfire StoreSafe iSCSI virtual storage at Windows Server 2008 or Linux with authorized IP network address with correct CHAP user authentication credentials

yields successful connection to Bloombase Spitfire StoreSafe iSCSI virtual storage target. Otherwise, access denied.

2.3.5 Mount Bloombase Spitfire StoreSafe iSCSI virtual storage

Mount Bloombase Spitfire StoreSafe iSCSI virtual storage as local storage device.

Example Use Case: Mount Bloombase Spitfire StoreSafe iSCSI virtual storage target at Windows Server 2008 or Linux with authorized IP network address with correct CHAP user authentication credentials yields successful connection to Bloombase Spitfire StoreSafe iSCSI virtual storage and be able to access as local block device at /dev/sdx on UNIX or new hard drive at Windows disk management tool.

2.3.6 Write and encrypt contents at Bloombase Spitfire StoreSafe iSCSI virtual storage as raw storage device

Write and dump in contents to Bloombase Spitfire StoreSafe iSCSI virtual storage as raw storage device and gets encrypted and persisted physically at Dell Equallogic.

Example Use Case: Dump contents at mounted Bloombase Spitfire StoreSafe iSCSI virtual storage target at Windows Server 2008 or Linux with authorized IP network address with correct CHAP user authentication credentials as raw storage device as if normal virtual-plain raw storage device. Grep for plain contents at physical Dell Equallogic iSCSI target using dd and should yield nothing because entire raw storage device get fully encrypted by Bloombase Spitfire StoreSafe.

2.3.7 Read and un-encrypt contents at Bloombase Spitfire StoreSafe iSCSI virtual storage as raw storage device

Read and dump out contents from Bloombase Spitfire StoreSafe iSCSI virtual storage as raw storage device and gets un-encrypted and retrieved physically from Dell Equallogic.

Example Use Case: Read and dump out contents at mounted Bloombase Spitfire StoreSafe iSCSI virtual storage target at Windows Server 2008 or Linux with authorized IP network address with correct CHAP user authentication credentials as raw storage device as if normal virtual-plain contents.

2.3.8 Format Bloombase Spitfire StoreSafe iSCSI virtual storage as local file system

Format Bloombase Spitfire StoreSafe iSCSI virtual storage and access as local file system.

Example Use Case: Format mounted Bloombase Spitfire StoreSafe iSCSI virtual storage target at Windows Server 2008 or Linux with authorized IP network address with correct CHAP user authentication credentials as NTFS or ext3 respectively and assign drive letter or local mount point enabling access of Bloombase Spitfire StoreSafe iSCSI virtual storages as local file system resources.

2.3.9 Store and encrypt contents at Bloombase Spitfire StoreSafe iSCSI virtual storage via local file system

Store files and contents at Bloombase Spitfire StoreSafe iSCSI virtual storage as local file system and gets encrypted and persisted physically at Dell Equallogic.

Example Use Case: Create and store files or folders at mounted Bloombase Spitfire StoreSafe iSCSI virtual storage target at Windows Server 2008 or Linux with authorized IP network address with correct CHAP user authentication credentials as local file system as if normal virtual-plain files and folders. Grep for plain contents at physical Dell Equallogic iSCSI target using dd and should yield nothing because entire file systems get fully encrypted by Bloombase Spitfire StoreSafe.

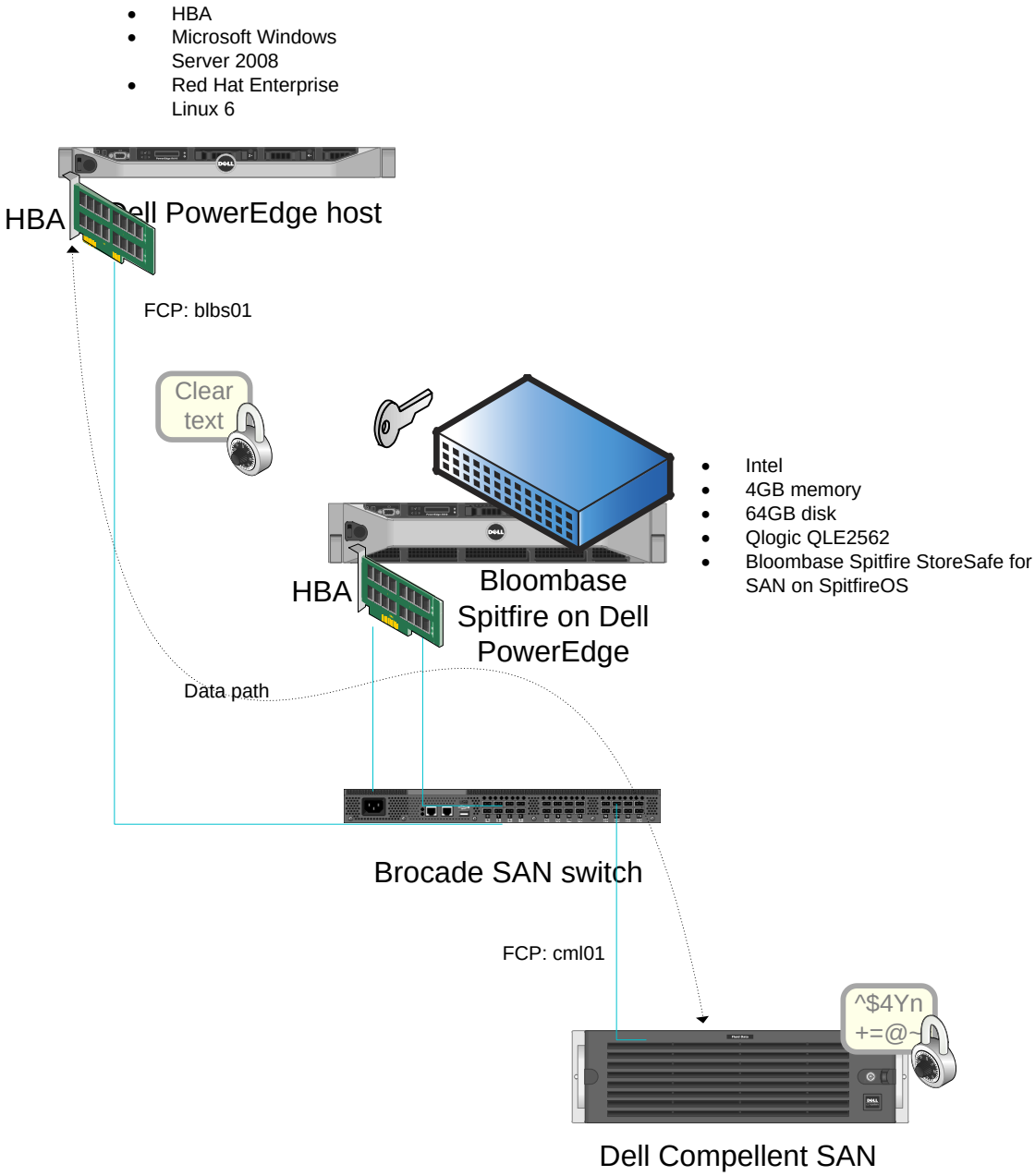
2.3.10 Retrieve and un-encrypt contents at Bloombase Spitfire StoreSafe iSCSI virtual storage via local file system

Retrieve files and contents at Bloombase Spitfire StoreSafe iSCSI virtual storage as local file system and gets un-encrypted and retrieved physically from Dell Equallogic.

Example Use Case: Access and read files or folders at mounted Bloombase Spitfire StoreSafe iSCSI virtual storage target at Windows Server 2008 or Linux with authorized IP network address with correct CHAP user authentication credentials as local file system as if normal virtual-plain files and folders.

2.4 Use Cases for Compellent as the storage device for FC-SAN security

The Use Cases for supporting Compellent as the storage system for FC-SAN security with PowerEdge server for Bloombase solution.



- HBA
- Microsoft Windows Server 2008
- Red Hat Enterprise Linux 6

2.4.1 LUN masking access control

Only authorized hosts are allowed to access Bloombase Spitfire StoreSafe FC-SAN virtual storage targets.

Example Use Case: Access Bloombase Spitfire StoreSafe FC-SAN virtual storage at Windows Server 2008 or Linux with authorized HBA WWNs and proper SAN switch zoning yields successful connection to Bloombase Spitfire StoreSafe FC-SAN virtual storage. Otherwise, access denied.

2.4.2 Bloombase Spitfire StoreSafe FC-SAN virtual storage target connection

Connect and access Bloombase Spitfire StoreSafe FC-SAN virtual storage targets.

Example Use Case: Access Bloombase Spitfire StoreSafe FC-SAN virtual storage at Windows Server 2008 or Linux with authorized HBA WWNs and proper SAN switch zoning yields successful connection to Bloombase Spitfire StoreSafe FC-SAN virtual storage target. Otherwise, access denied.

2.4.3 Mount Bloombase Spitfire StoreSafe FC-SAN virtual storage

Mount Bloombase Spitfire StoreSafe FC-SAN virtual storage as local storage device.

Example Use Case: Mount Bloombase Spitfire StoreSafe FC-SAN virtual storage target at Windows Server 2008 or Linux with authorized HBA WWNs and proper SAN switch zoning yields successful connection to Bloombase Spitfire StoreSafe iSCSI virtual storage and be able to access as local block device at /dev/sdx on UNIX or new hard drive at Windows disk management tool.

2.4.4 Write and encrypt contents at Bloombase Spitfire StoreSafe FC-SAN virtual storage as raw storage device

Write and dump in contents to Bloombase Spitfire StoreSafe FC-SAN virtual storage as raw storage device and gets encrypted and persisted physically at Dell Compellent.

Example Use Case: Dump contents at mounted Bloombase Spitfire StoreSafe FC-SAN virtual storage target at Windows Server 2008 or Linux with authorized HBA WWNs and proper SAN switch zoning as raw storage device as if normal virtual-plain raw storage device. Grep for plain contents at physical Dell Compellent FC-SAN target using dd

and should yield nothing because entire raw storage device get fully encrypted by Bloombase Spitfire StoreSafe.

2.4.5 Read and un-encrypt contents at Bloombase Spitfire StoreSafe FC-SAN virtual storage as raw storage device

Read and dump out contents from Bloombase Spitfire StoreSafe FC-SAN virtual storage as raw storage device and gets un-encrypted and retrieved physically from Dell Compellent.

Example Use Case: Read and dump out contents at mounted Bloombase Spitfire StoreSafe FC-SAN virtual storage target at Windows Server 2008 or Linux with authorized HBA WWNs and proper SAN switch zoning as raw storage device as if normal virtual-plain contents.

2.4.6 Format Bloombase Spitfire StoreSafe FC-SAN virtual storage as local file system

Format Bloombase Spitfire StoreSafe FC-SAN virtual storage and access as local file system.

Example Use Case: Format mounted Bloombase Spitfire StoreSafe FC-SAN virtual storage target at Windows Server 2008 or Linux with authorized HBA WWNs and proper SAN switch zoning as NTFS or ext3 respectively and assign drive letter or local mount point enabling access of Bloombase Spitfire StoreSafe FC-SAN virtual storages as local file system resources.

2.4.7 Store and encrypt contents at Bloombase Spitfire StoreSafe FC-SAN virtual storage via local file system

Store files and contents at Bloombase Spitfire StoreSafe FC-SAN virtual storage as local file system and gets encrypted and persisted physically at Dell Compellent.

Example Use Case: Create and store files or folders at mounted Bloombase Spitfire StoreSafe FC-SAN virtual storage target at Windows Server 2008 or Linux with authorized HBA WWNs and proper SAN switch zoning as local file system as if normal virtual-plain files and folders. Grep for plain contents at physical Dell Compellent FC-SAN target using dd and should yield nothing because entire file systems get fully encrypted by Bloombase Spitfire StoreSafe.

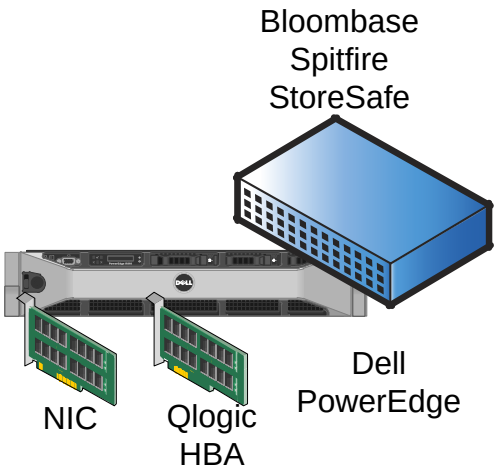
2.4.8 Retrieve and un-encrypt contents at Bloombase Spitfire StoreSafe FC-SAN virtual storage via local file system

Retrieve files and contents at Bloombase Spitfire StoreSafe FC-SAN virtual storage as local file system and gets un-encrypted and retrieved physically from Dell Compellent.

Example Use Case: Access and read files or folders at mounted Bloombase Spitfire StoreSafe FC-SAN virtual storage target at Windows Server 2008 or Linux with authorized HBA WWNs and proper SAN switch zoning as local file system as if normal virtual-plain files and folders.

2.5 The Bloombase solution Configuration

This section covers the configuration of the solution with detailed hardware requirement and set up, and GUI for any required configuration.



Bloombase Spitfire StoreSafe v3.5 ISO is to be installed at Dell PowerEdge server providing agentless non-disruptive file-based, block-based and object-based encryption of at-rest data managed at Dell Equallogic NAS, Compellent SAN, and DX object stores.

For NAS applications with Dell Equallogic, only network interface cards (NIC) are required.

For SAN applications with Dell Compellent, additionally, it requires the presence of QLogic host bus adapters (HBA).

2.5.1 Parameters for configuration

Bloombase Spitfire StoreSafe Network Configuration

- Host name: blbs01
- IP address: 10.10.10.141

Bloombase Spitfire StoreSafe NAS Server Configuration

- SMB server name: blbs01

Bloombase Spitfire StoreSafe SAN Server Configuration

- Targets: <WWNs of HBAs which act as target>

Bloombase Spitfire StoreSafe Key Management

- Key name: key01
- Bit length: 1024

Bloombase Spitfire StoreSafe CIFS Configuration

- Virtual storage name: cifs01
- Type: File/Share
- Physical storage: \\eqlx01\cifs01
- Protection: Privacy
- Key: key01
- Cipher algorithm: AES
- Key length: 256
- User access control: user01/123456
- Host access control: 10.10.10.140

Bloombase Spitfire StoreSafe NFS Configuration

- Virtual storage name: nfs01
- Type: File/Share
- Physical storage: eqlx01:/nfs01
- Protection: Privacy
- Key: key01

- Cipher algorithm: AES
- Key length: 256
- Host access control: 10.10.10.140

Bloombase Spitfire StoreSafe iSCSI Configuration

- Virtual storage name: iqn.2004-11.com.bloombase:blbs01-iscsi01
- Type: iSCSI
- Physical storage: 192.168.0.2:3260/iqn. 2001-5.com.equallogic:0-8a0906-f1f58150c-67c446208064fc91-bloombaseeqliscsi
- Protection: Privacy
- Key: key01
- Cipher algorithm: AES
- Key length: 256
- User access control: user01/123456
- Host access control: 10.10.10.140

Bloombase Spitfire StoreSafe FC-SAN Configuration

- Virtual storage name: san01
- Type: FC-SAN
- Physical storage: <as presented to Bloombase Spitfire StoreSafe)
- Protection: Privacy
- Key: key01
- Cipher algorithm: AES
- Key length: 256
- Host access control: <WWNs of HBA at host>

2.5.2 Configuration Screens

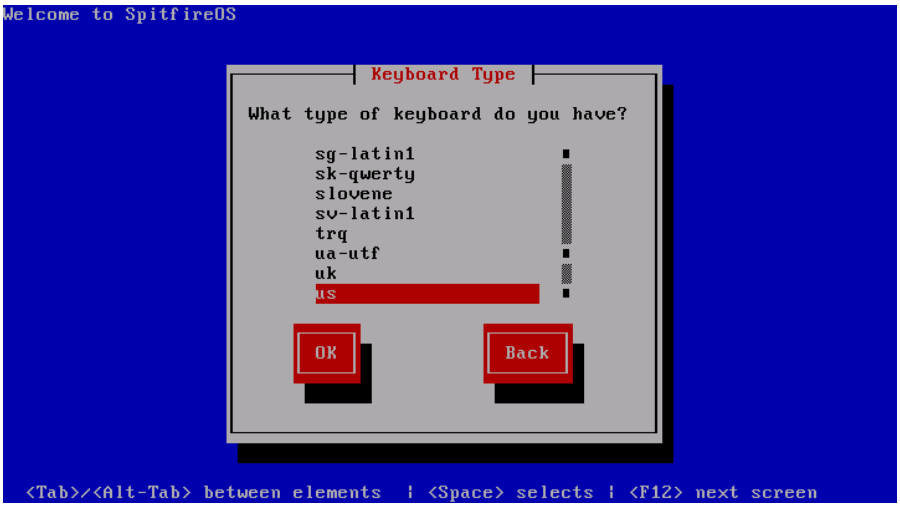
Installation

Bloombase Spitfire Server ISO images can be directly mounted as virtual disk drive on VMware Server or ESX for virtual appliance installation.
Or they are available as installation CD/DVD to be installed directly from disk drives.

Bloombase SpitfireOS installer will guide you through the rest of the installation process.

Keyboard Configuration

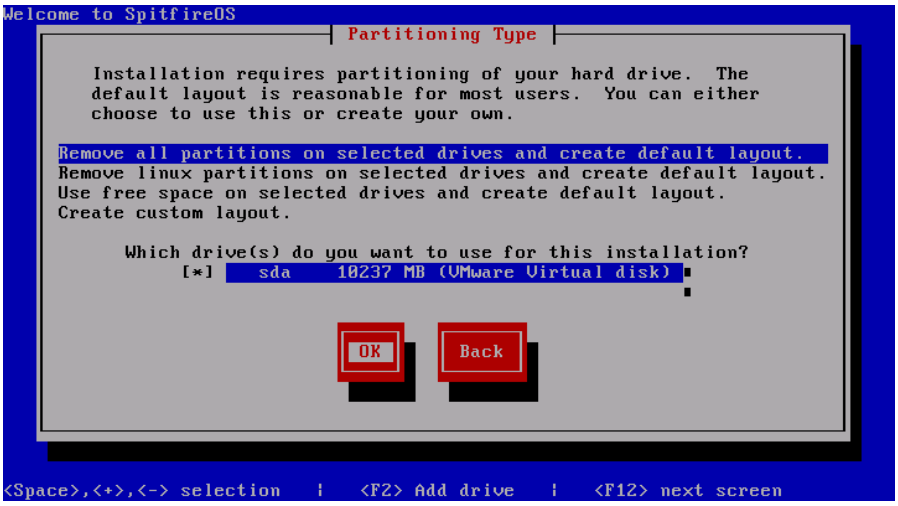
Choose the type of keyboard that is attached to the physical or virtual appliance on which Bloombase Spitfire Server is installed. As a default option, select keyboard type as ‘us’.



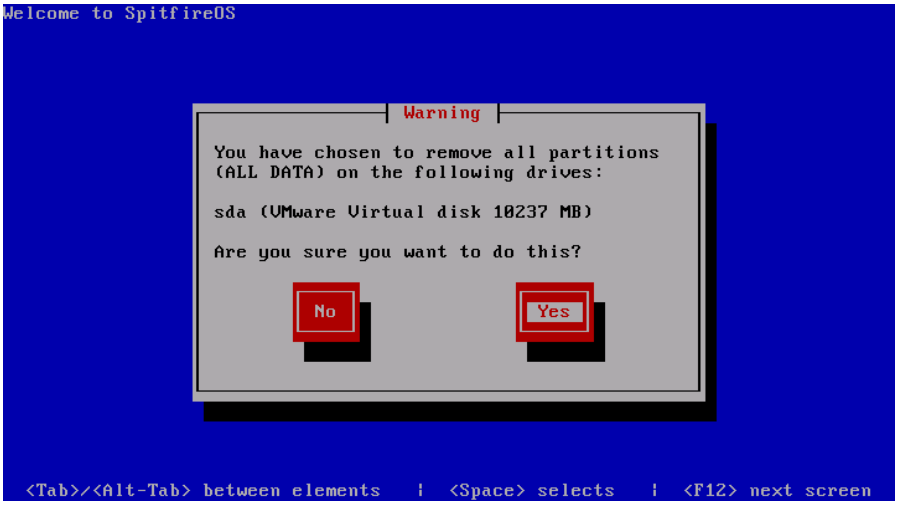
Disk Partitioning

Attached hard-drive partition table has to be erased before Bloombase SpitfireOS installer starts to install.
Press ‘Yes’ to confirm if the partition table can be erased.

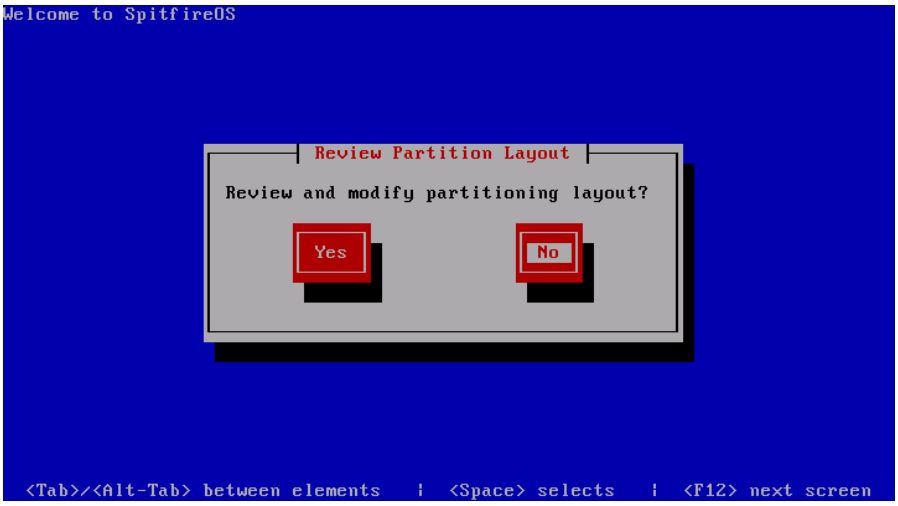
Specify the layout of disk partitioning that is good for the installation of Bloombase Spitfire Server.
Select the partition where Bloombase SpitfireOS is to be installed at.
Push ‘OK’ to continue.



Bloombase SpitfireOS prompts again to confirm if SpitfireOS is to be deployed and installed in the specified hard drive partition.
Press ‘Yes’ to double confirm.

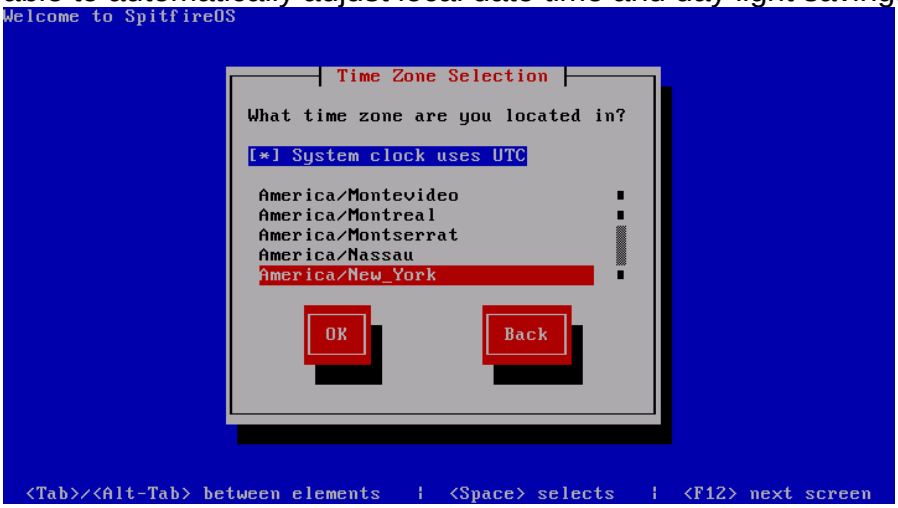


Bloombase SpifireOS prompts to review partition table and if any modifications are required.
If you are sure of the partitioning settings, simply push ‘No’ button when prompted.



System Time Zone Configuration

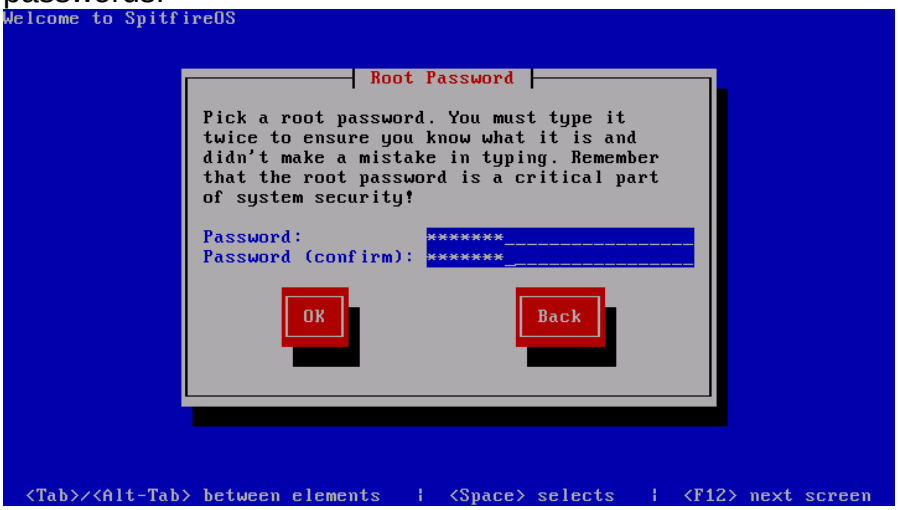
Specify Bloombase SpitfireOS to use UTC for system clock. Configure the location where Bloombase Spitfire Server serves, this step is important especially for time sensitive applications such as time stamping.
Once time zone is properly configured, Bloombase SpitfireOS is able to automatically adjust local date time and day light saving.



Bloombase SpitfireOS Super User Configuration

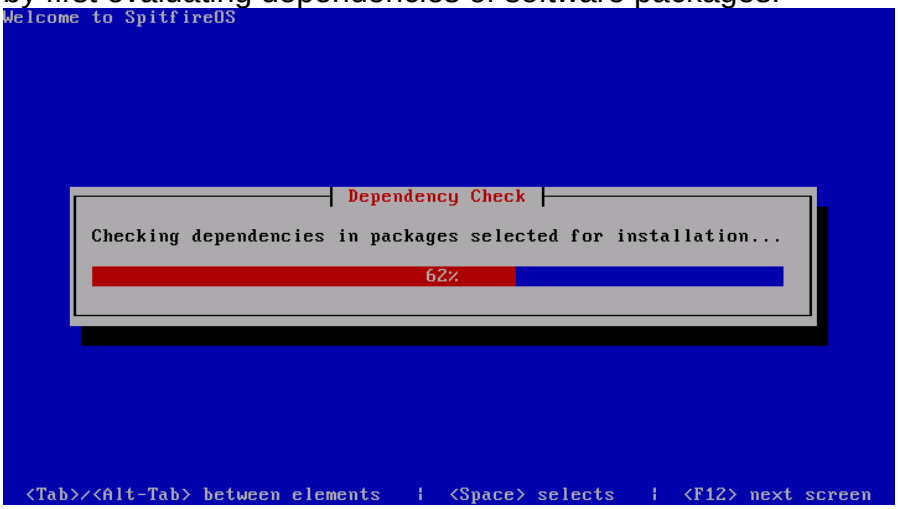
Under normal usage, customers do not require to access to SpitfireOS. Administrators, operators, and users can simply utilize command line interface (CLI) console and web management console for administration and management.
For circumstances where unsupported or special hardware has to be added to the system, administrators might have to get super

user or root access to SpitfireOS to get hardware drivers installed, configured and provisioned.
Specify a SpitfireOS root password when prompted.
IMPORTANT: SpitfireOS super user password empowers administrator to gain system root access to SpitfireOS. Customers should handle SpitfireOS super user password with great care and secrecy as much as their CLI and web management console passwords.

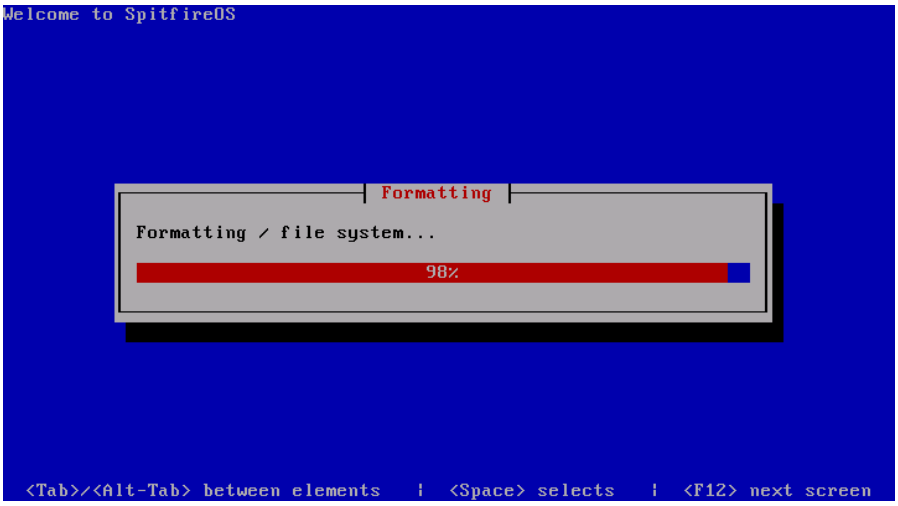


SpitfireOS Operating System Installation

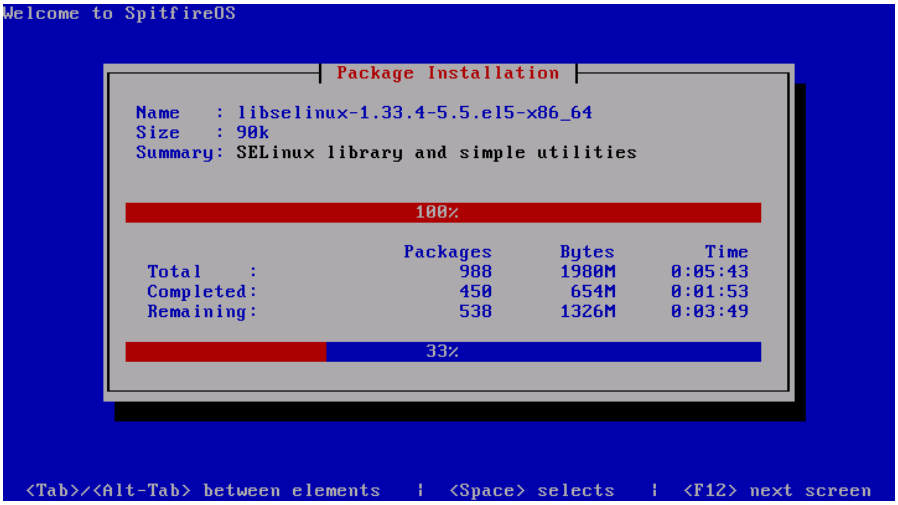
SpitfireOS automatic installer deploys the software on the system by first evaluating dependencies of software packages.



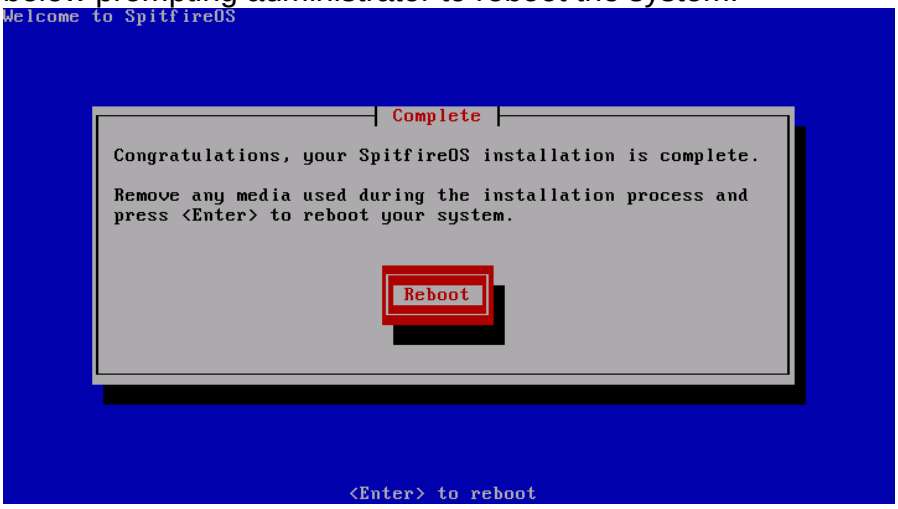
SpitfireOS starts to format the specified hard drive location and builds up the required file system.



SpitfireOS delivers baseline software packages to the operating system that is required to power application specific Spitfire Servers.

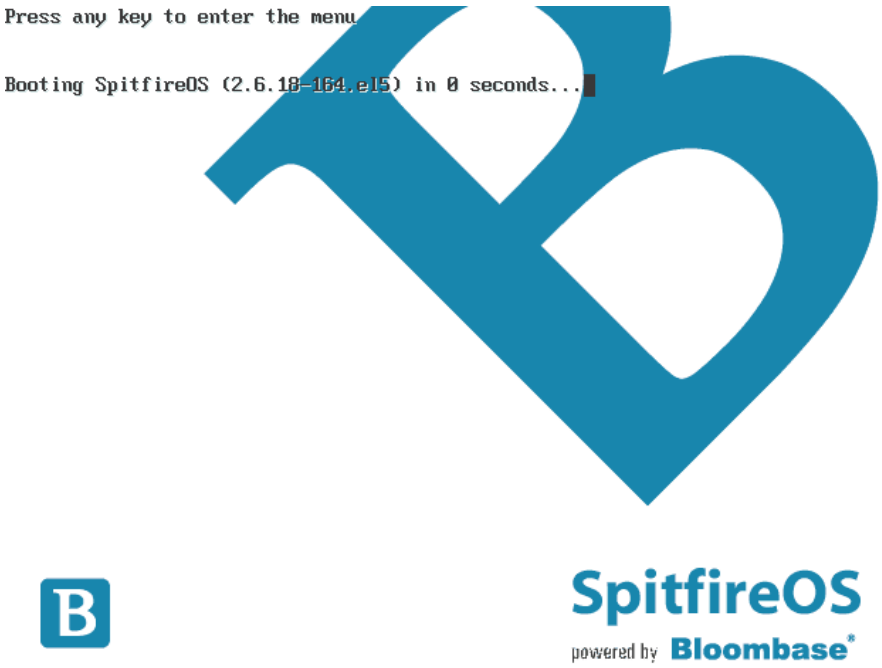


Once SpitfireOS successfully deploys a dialog will be shown as below prompting administrator to reboot the system.



Follow instructions to restart the newly deployed system.

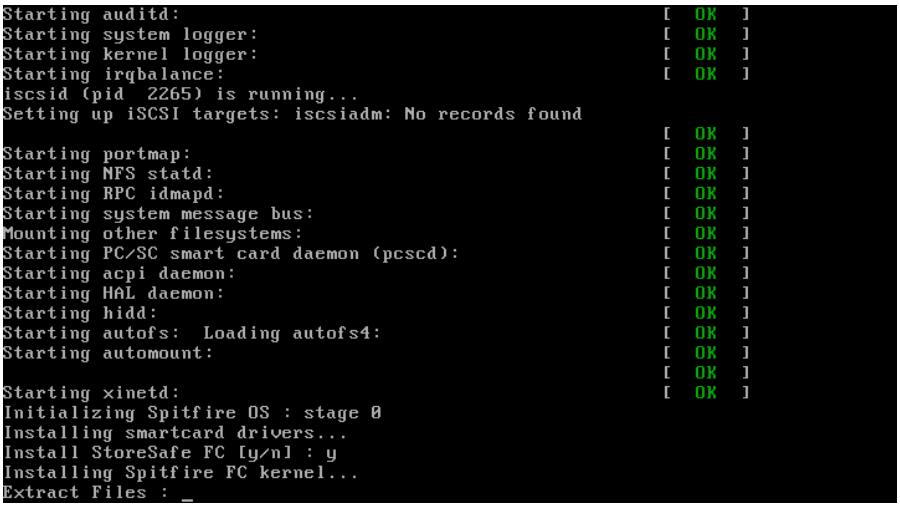
Post Installation Procedures



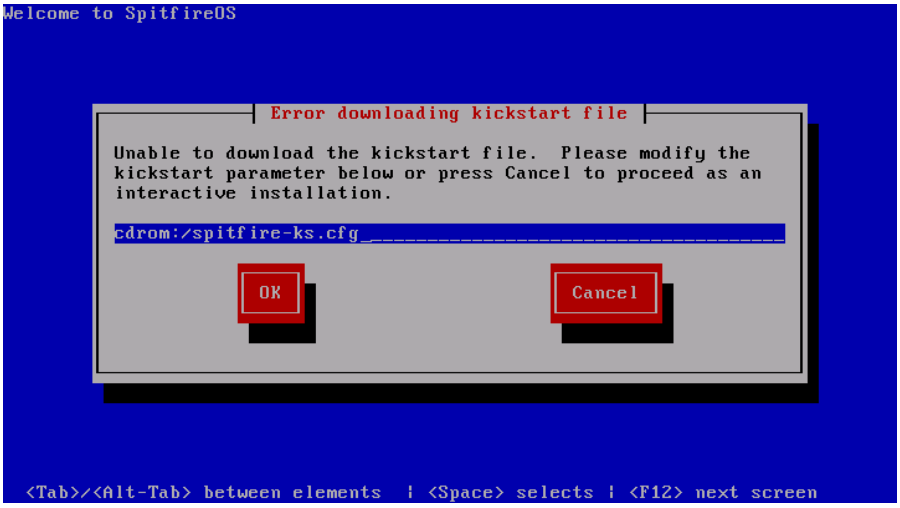
Bloombase SpitfireOS will boot up for the first time and completes the rest of post-installation procedure, if any.

```
Determining IP information for eth0... done.
                                                           [  OK  ]
Starting auditd:                                           [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]
Starting irqbalance:                                       [  OK  ]
iscsid (pid  2265) is running...
Setting up iSCSI targets: iscsiadm: No records found
                                                           [  OK  ]
Starting portmap:                                          [  OK  ]
Starting NFS statd:                                        [  OK  ]
Starting RPC idmapd:                                       [  OK  ]
Starting system message bus:                               [  OK  ]
Mounting other filesystems:                                [  OK  ]
Starting PC/SC smart card daemon (pcscd):                  [  OK  ]
Starting acpi daemon:                                      [  OK  ]
Starting HAL daemon:                                       [  OK  ]
Starting hidd:                                             [  OK  ]
Starting autofs:  Loading autofs4:                         [  OK  ]
Starting automount:                                        [  OK  ]
                                                           [  OK  ]
Starting xinetd:                                           [  OK  ]
Initializing Spitfire OS : stage 0
Installing smartcard drivers...
Install StoreSafe FC [y/n] : _
```

You will be prompted to install additional components and software modules as required by Spitfire Server, answer ‘y’ to start the rest of software installation.



There are occasions that the URL to Spitfire kickstart file location is wrongly positioned or simply the device name of CD ROM is not of default ‘cdrom’.



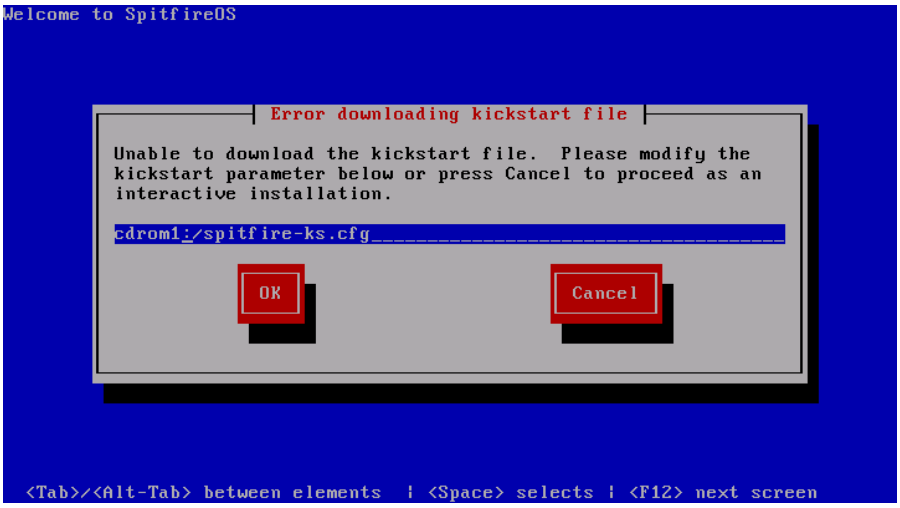
In this case, simply alter URL from

cdrom:/spitfire-ks.cfg

to

cdrom1:/spitfire-ks.cfg

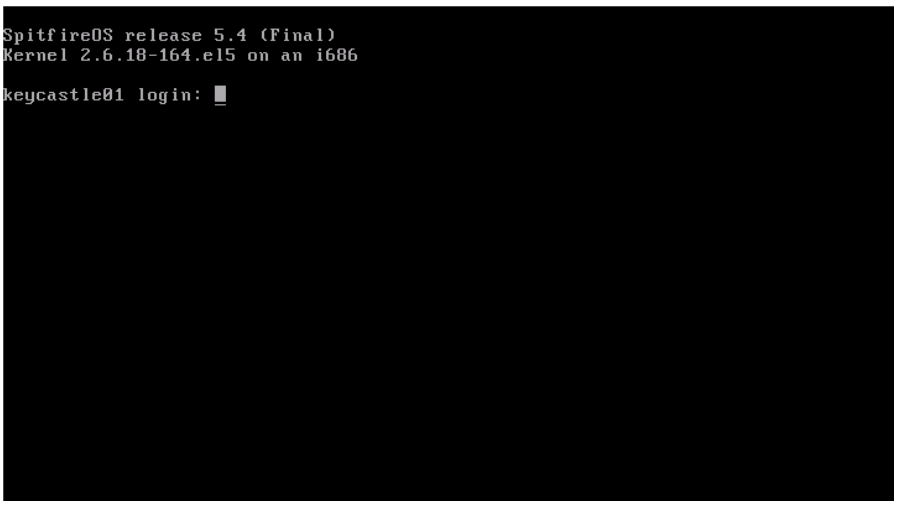
If this does not fix, try cdrom2, cdrom3, etc until the installer can proceed with the rest of installation.



On completion of SpitfireOS installation, Spitfire server installer will kick in and start deploying Spitfire server binaries to get the application specific Spitfire server and related components installed and setup.
SpitfireOS might prompt to reboot system one more time if any system related packages have been deployed.

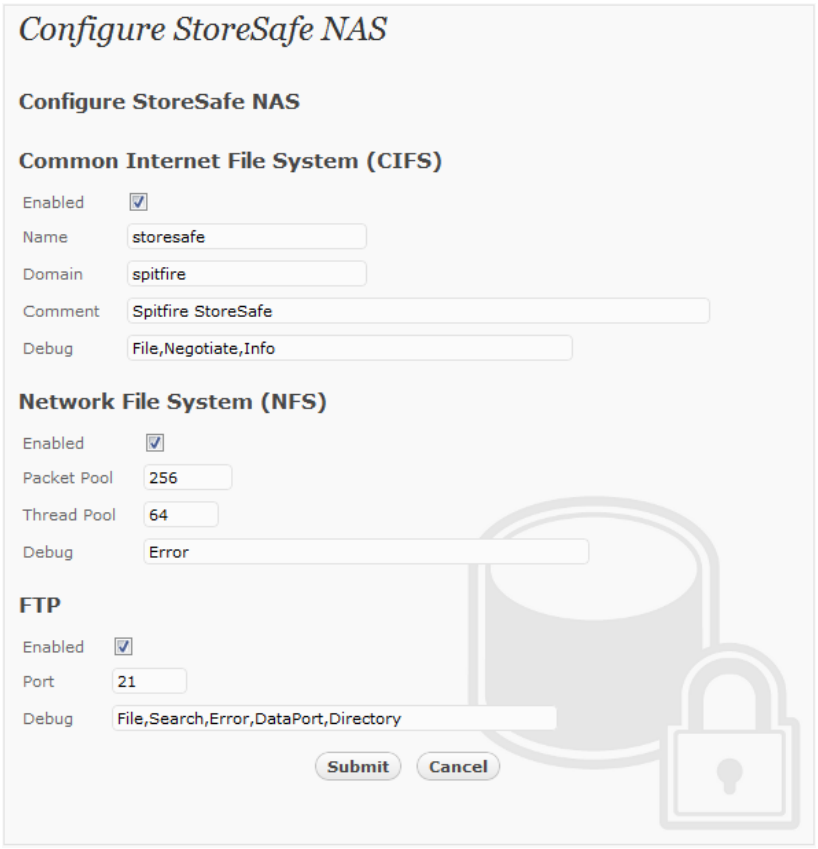
```
Starting portmap:                                          [  OK  ]
Starting NFS statd:                                        [  OK  ]
Starting RPC idmapd:                                       [  OK  ]
Starting system message bus:                               [  OK  ]
Mounting other filesystems:                                [  OK  ]
Starting PC/SC smart card daemon (pcscd):                  [  OK  ]
Starting acpi daemon:                                      [  OK  ]
Starting HAL daemon:                                       [  OK  ]
Starting hidd:                                             [  OK  ]
Starting autofs:  Loading autofs4:                         [  OK  ]
Starting automount:                                        [  OK  ]
                                                           [  OK  ]
Starting xinetd:                                           [  OK  ]
Initializing Spitfire OS : stage 0
Installing smartcard drivers...
Install StoreSafe FC [y/n] : y
Installing Spitfire FC kernel...
Extract Files : DONE
Compile Spitfire FC kernel : DONE
Compile Spitfire FC kernel modules :
DONE
Install Spitfire FC kernel : DONE
Init Setup stage 0 done, reboot required
Reboot in 30s
Input 'x' to abort : _
```

Once Spitfire Server completes installation and reboot the second time, you will see login prompt to the Spitfire CLI console.
The Spitfire Server is ready for configuration and to serve.

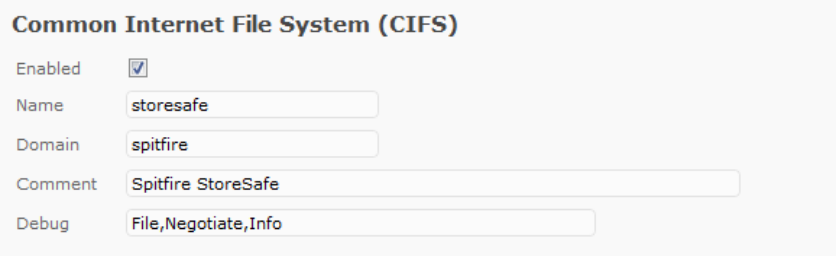


NAS Server Configuration

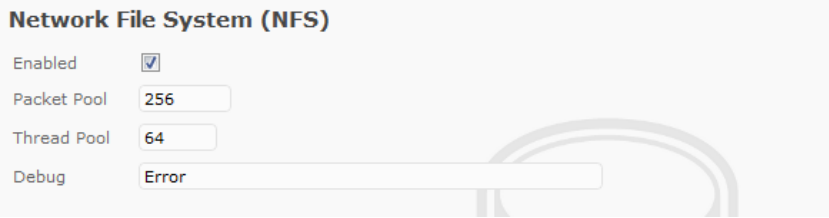
To configure Spitfire StoreSafe NAS service components, StoreSafe administrator can sign on StoreSafe web-based management console. Expand ‘Storage’ menu and launch ‘Configure StoreSafe NAS’ tool.



For CIFS



For NFS

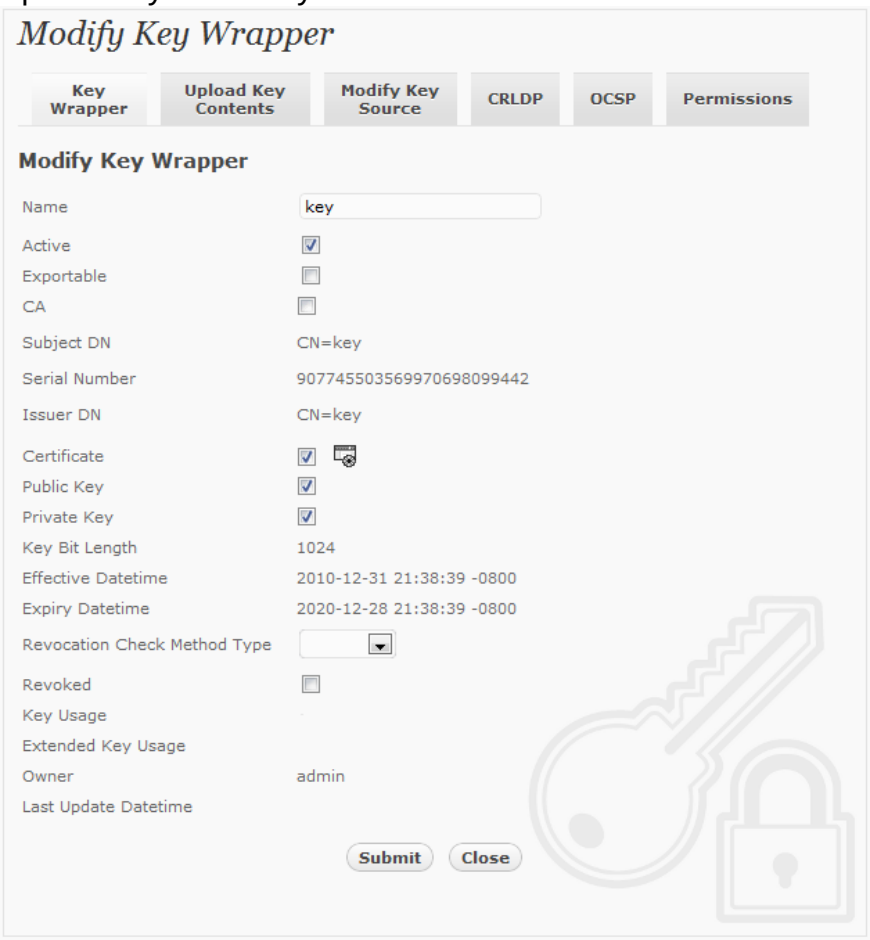


SAN Server Configuration

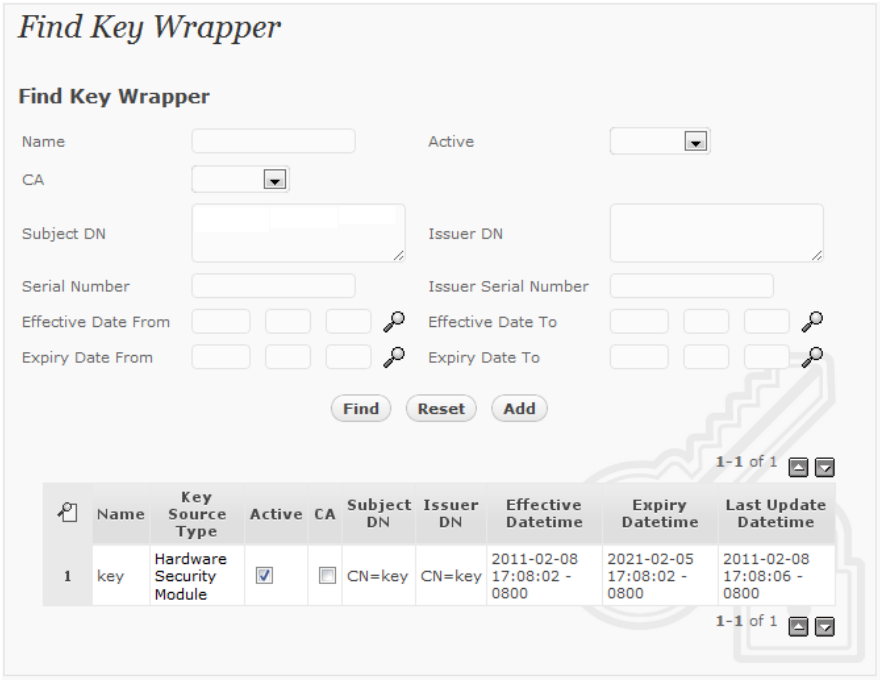
Navigate ‘Storage’ menu and launch ‘Configure StoreSafe SAN’ tool to enter the list of fiber channel SAN targets provided by Spitfire StoreSafe SAN module for servers equipped with compatible fiber channel host bus adapters (HBA).

Key Management

Push ‘Generate’ button to invoke key generation in the specified HSM. Depending on performance of the HSM, key generation might take relatively longer time than normal software-based Spitfire KeyCastle keys.



Double check everything are alright. Push ‘Submit’ button to commit changes to Bloombase Spitfire KeyCastle.
Verify HSM key by invoking ‘Find Key Wrapper’ function.

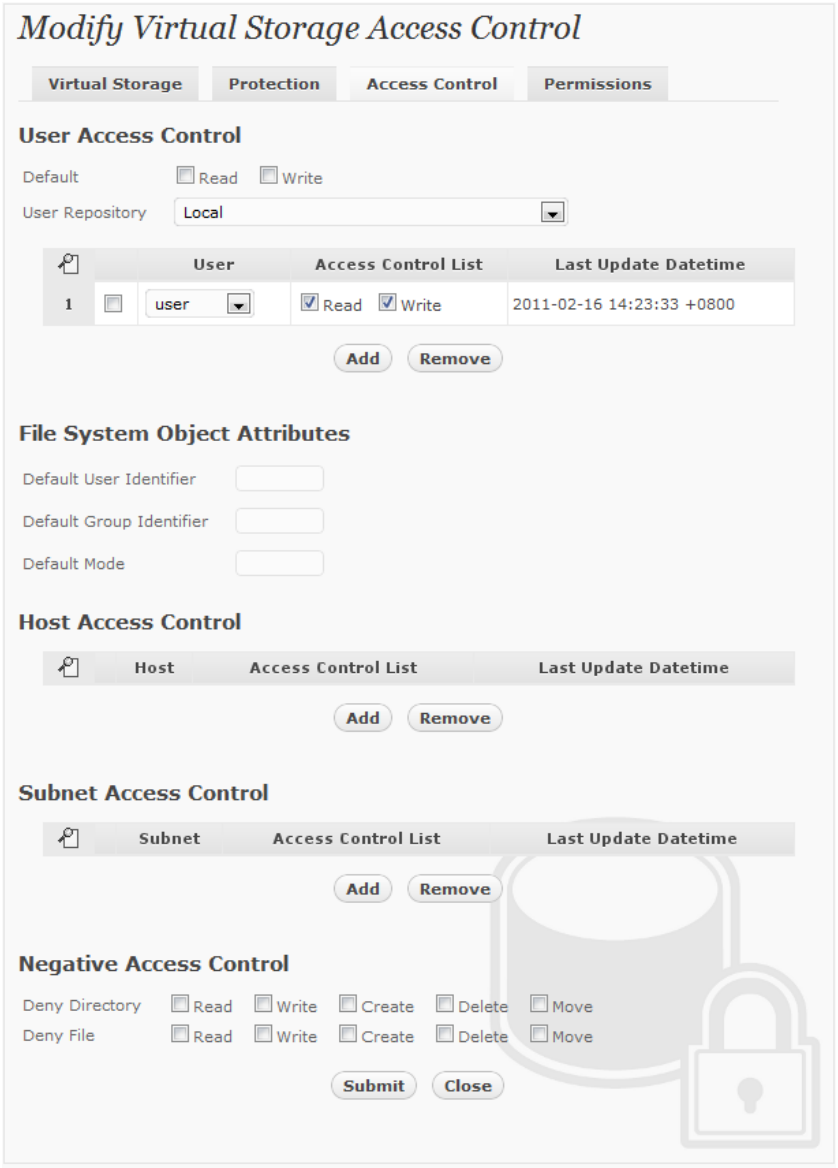


CIFS Virtual Storage Configuration

Navigate Storage left menu and click 'Virtual Storage' tool. Push 'Add' button to create virtual storage for interception of sensitive file storage to physical storage named 'cifs01'
Name the virtual storage as ‘cifs01'. Select virtual storage mode as 'File' or ‘Share’ which means file-based protection. File-based protection is more secure than secure whereas share-based protection enables effective deduplication and compression. Pick 'cifs01' as physical storage. Virtual storage 'cifs01' will be created as a network share to be accessed by a Windows client to be detailed in later part of this section.

Turn to 'Virtual Storage Handler' tab and specify protection as 'Privacy' which means encryption has to be applied onto the virtual storage resources.

Secure files inside cifs01 by AES-256 bit cipher encrypted by 'key01' previously generated.



Turn to 'Storage Access Control' tab and allow all hosts in the same network to access the Spitfire StoreSafe secured storage, grant 'user01' the privilege to be able to access and write to the virtual storage.

Push 'Submit' button to commit changes.

NFS Virtual Storage Configuration

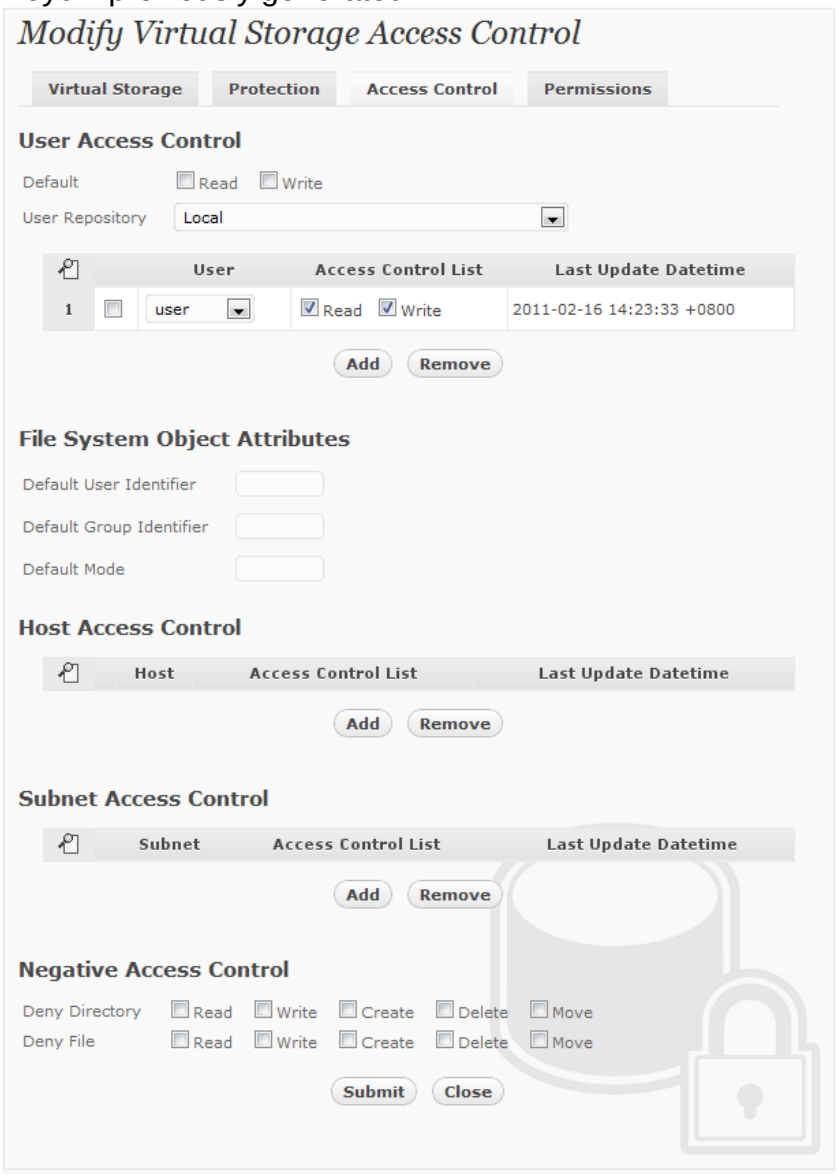
Navigate Storage left menu and click 'Virtual Storage' tool. Push 'Add' button to create virtual storage for interception of sensitive file storage to physical storage named 'nfs01'
Name the virtual storage as 'nfs01'. Select virtual storage mode as 'File' or 'Share' which means file-based protection. File-based protection is more secure than secure whereas share-based

protection enables effective deduplication and compression. Pick 'nfs01' as physical storage. Virtual storage 'nfs01' will be created as a network share to be accessed by a Windows client to be detailed in later part of this section.

Turn to 'Virtual Storage Handler' tab and specify protection as 'Privacy' which means encryption has to be applied onto the virtual storage resources.

Secure files inside nfs01 by AES-256 bit cipher encrypted by

'key01' previously generated.

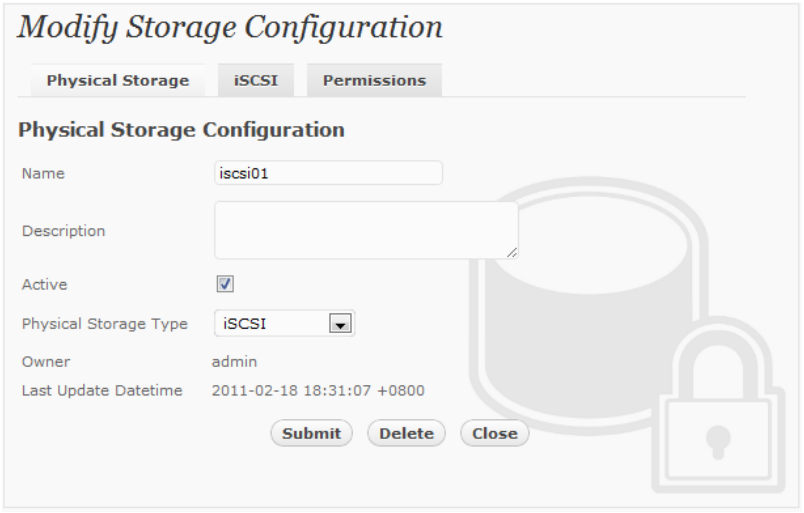


Turn to 'Storage Access Control' tab and allow all hosts in the same network to access the Spitfire StoreSafe secured storage, grant host IP the privilege to be able to access and write to the virtual storage.

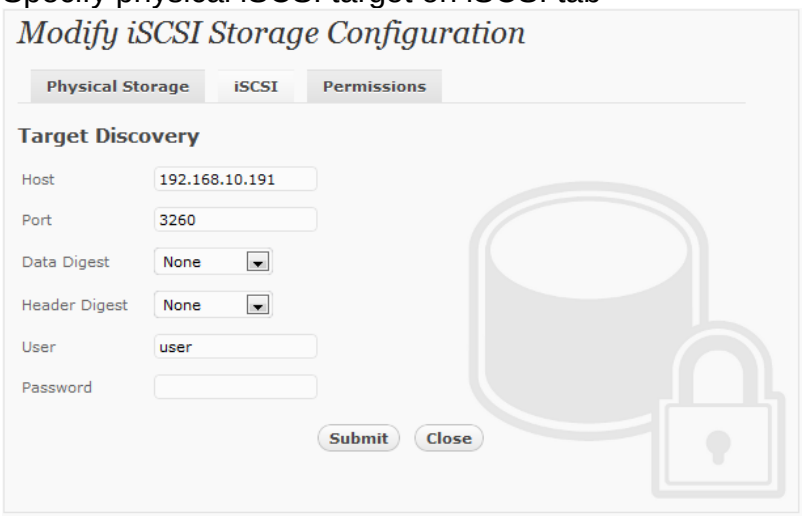
Push 'Submit' button to commit changes.

iSCSI Virtual Storage Configuration

Configure Spitfire StoreSafe to act as initiator to protect block-based iSCSI storage at Dell Equallogic and name the physical storage as ‘iscsi01’

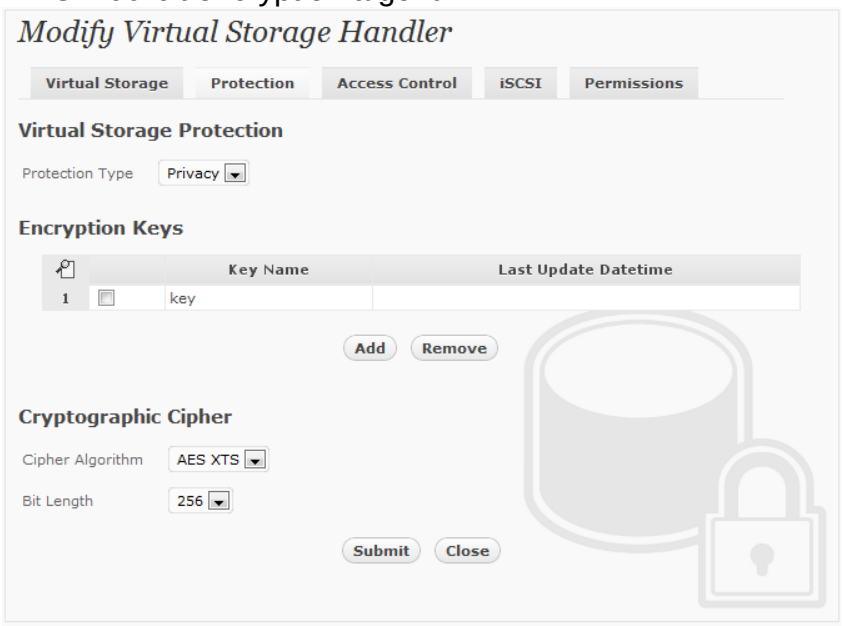


Specify physical iSCSI target on iSCSI tab

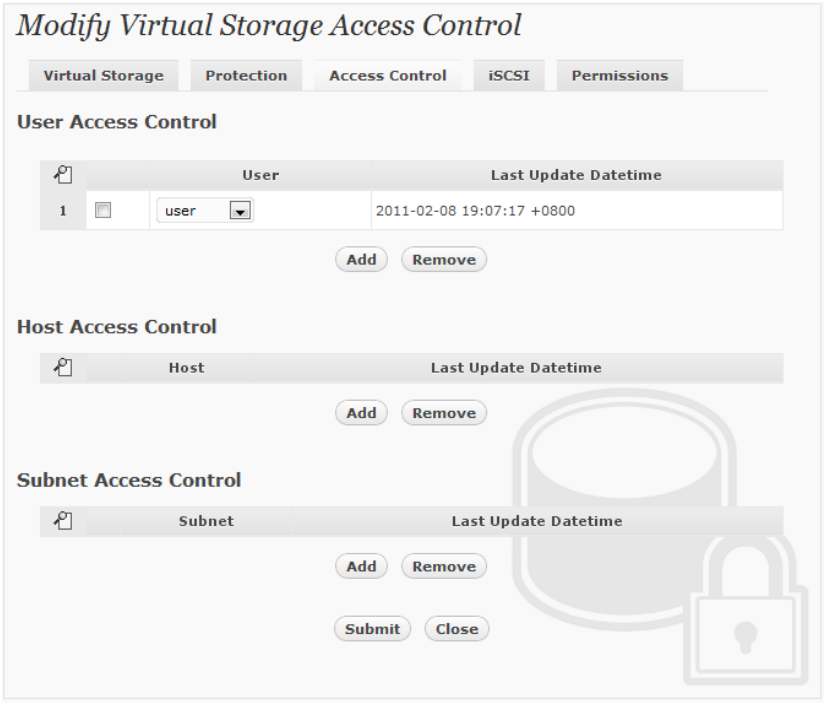


Create iSCSI-based virtual storage namely ‘iscsi01’ to virtualize actual iSCSI storage ‘iscsi01’

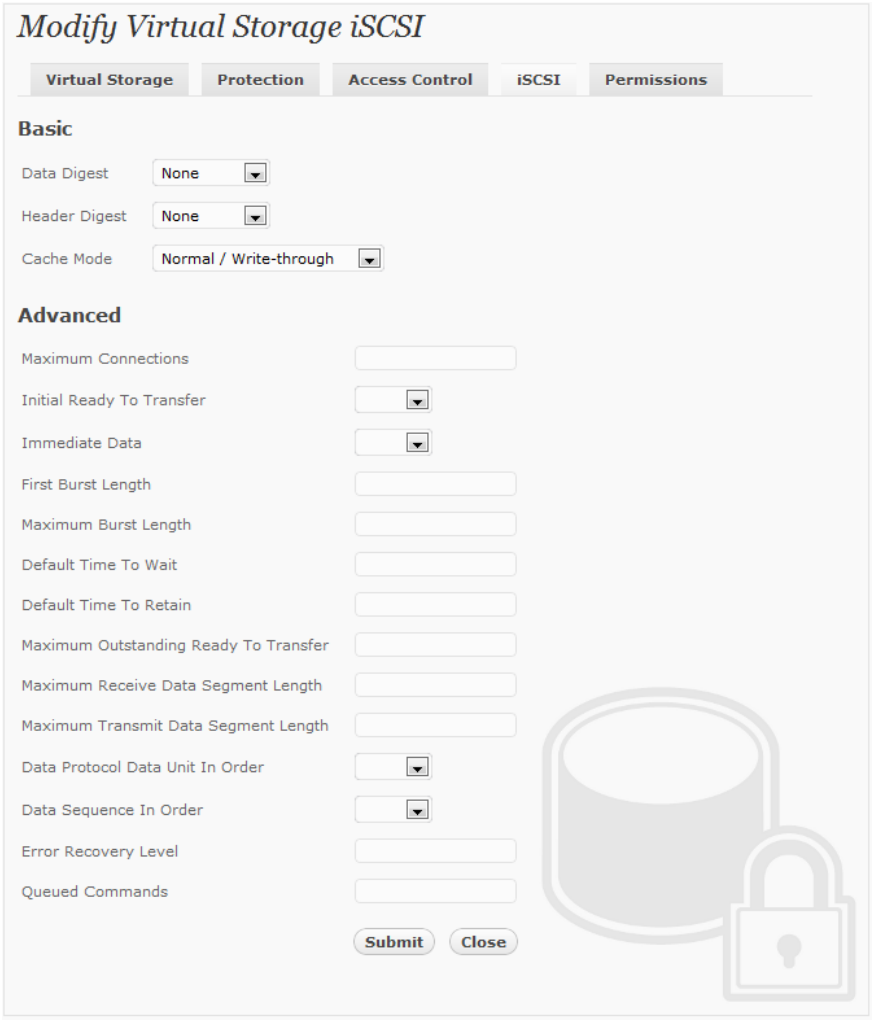
Protect contents of iSCSI storage by encryption key ‘key01’ using ‘AES’ 256-bit encryption algorithm



Enable user ‘user01’ to access virtual storage by adding to ‘User Access Control’ section of ‘Access Control’ tab

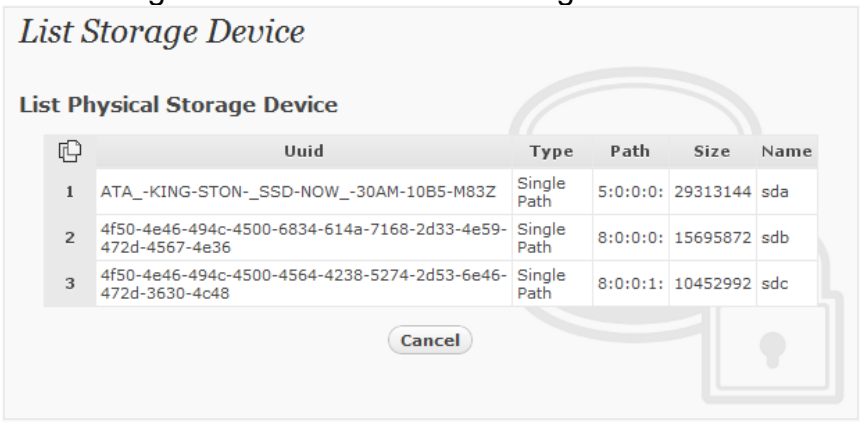


Further specify virtual storage iSCSI target attributes which are needed on ‘iSCSI’ tab

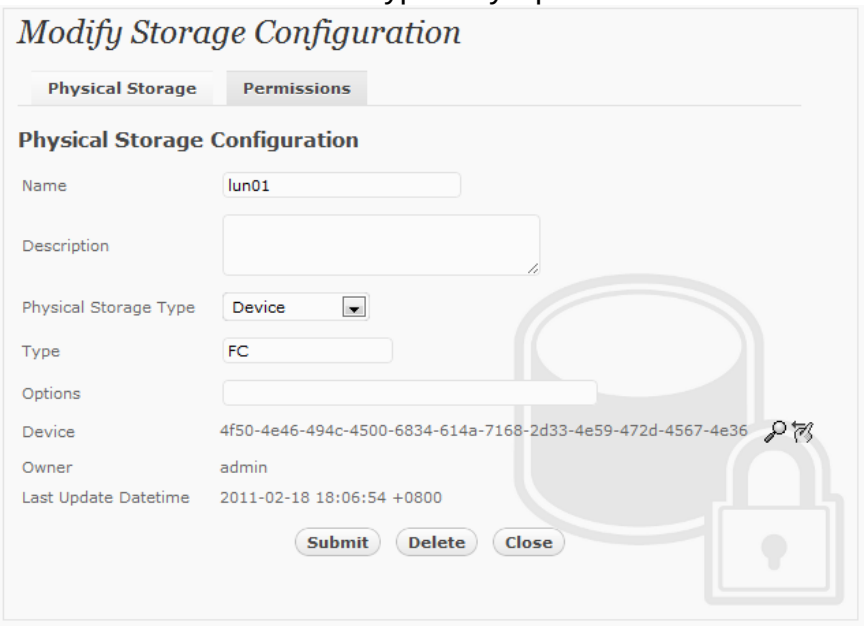


FC-SAN Virtual Storage Configuration

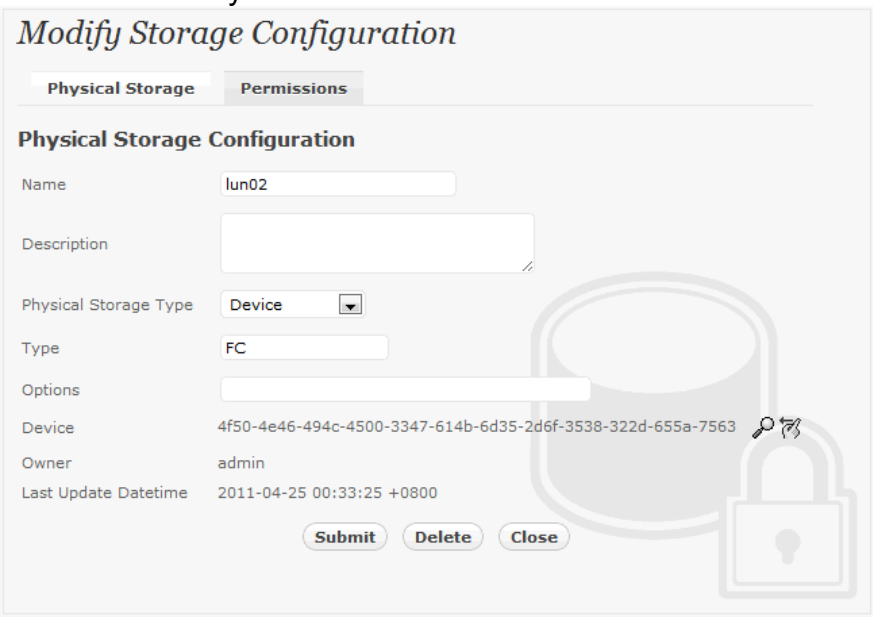
When zoning and LUN mask are properly configured at SAN switches, Spitfire StoreSafe should be able to mount to LUNs of SAN storages and shows on 'List Storage Device' tool.



Configure physical storage namely ‘san01’ to map to the storage device controller to be encrypted by Spitfire StoreSafe.



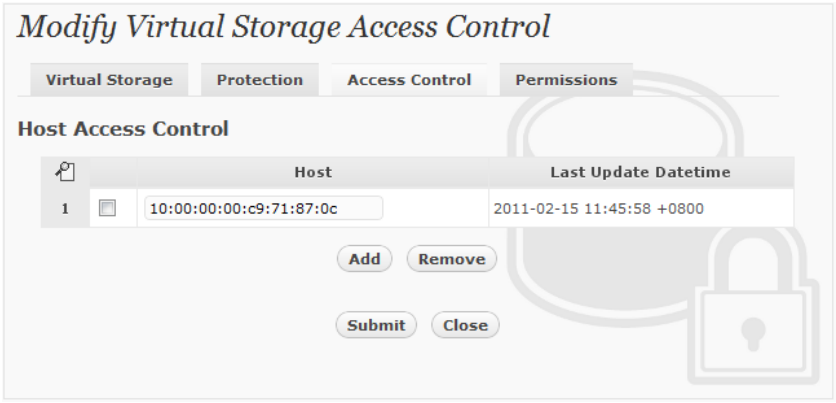
In most cases especially for enterprise scale deployment, there is more than one physical storage controller to map to the same volume in SAN.
Provision another physical storage for the second storage controller namely ‘san02’.



Create virtual storage namely ‘san01’ of type ‘FC’ to secure physical storages ‘san01’ and ‘san02’ for transparent encryption protection over FCP.

Specify protection type as ‘Privacy’ and secure the FC SAN LUN using AES-XTS 256-bit encryption with encryption key ‘key01’

Fiber channel protocol access control relies mainly on LUN mask for host based access control, specify the WWN of host HBA on ‘Host’ of ‘Host Access Control’ section as follows.
Add additional WWNs of host HBAs as required.



Press ‘Submit’ button to commit the newly provisioned SAN virtual storage.

3 Dell Storage Platform Certification

Certification of the Bloombase solution with the Dell Storage Platform including Equallogic and Compellent will be deemed complete and accepted by Dell when the Use Case designs in this document are demonstrated on a releasable version of the Bloombase solution.

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