SDC 20

BY Developers FOR Developers

Storage Developer Conference
September 22-23, 2020

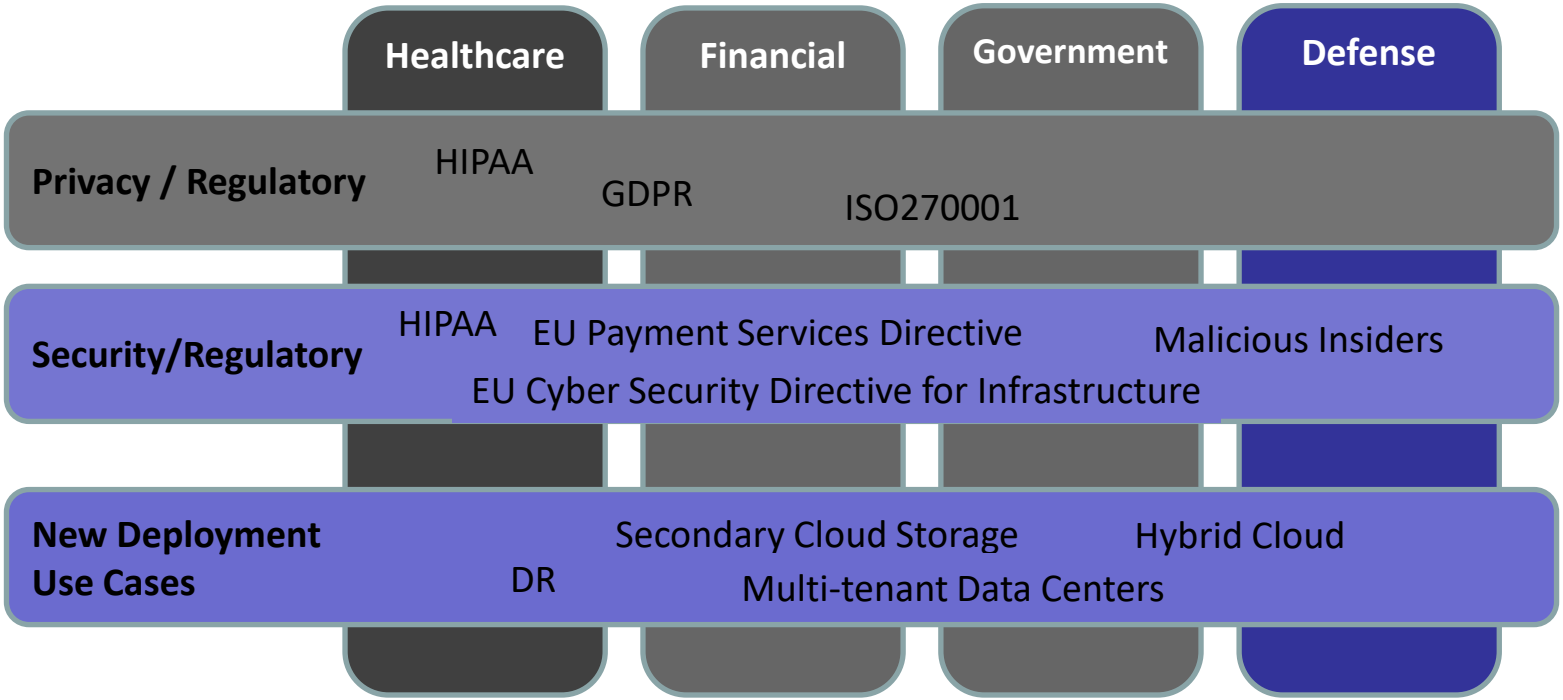
Encrypted FC at Wirespeed

Hannes Reinecke, SUSE
Nishant Lodha, Marvell

Encrypted FC at Wirespeed

- Industry trends driving data protection and security
- Potential Data Center Security Threats
- Data Security vs. Protection
- Implementing FC Encryption
- Marvell-SUSE Collaboration
- Next Steps

Drivers for Storage security



Isn’t FC Secure Already?

Trusted Storage Interconnect for Decades

Physical Security	• Data Centers are physically secured
Segregation	• Fibre Channel SANs are segregated networks
Partitioning	• FC Zoning ensures fabric partitioning
Masking	• LUN masking restricts access to specific LUNs
Management	• Out-of-Band Management (IP) is secure, OS Controls

Yes, But…

- New Data Center Architectures bring new threats
  - Distributed data centers - Remote replication and DR backups may be accessed by different users over Fabrics that span several sites
  - Multi Tenant data centers – Need to segregate and protect data traversing the same wire
- Increasing scale of FC SANs
  - Networks can be misconfigured
  - Fabric configuration databases are shared (not restricted to zones), have WKAs
- Existing mechanisms may not be enough
  - Switches are the sole entity that grant/deny access
    - Authorization based
  - “Segmentation” tools being used to implement “Security”
    - Soft zoning, LUN Masking

Potential DC Storage Security Threats

Sniffing Storage Traffic

Storage Masquerading

Data Corruption

Session Hijacking

Mitigated by Fibre Channel SAN Security

Data Protection vs. Security

- There is often confusion between storage/data security and protection.
- **Data security** refers specifically to measures taken to protect the integrity of the data itself.
- **Data security** primarily involves keeping private information out of the hands of anyone not authorized to see or modify it.
  - Unauthorized access
  - Intentional or accidental loss/corruption of sensitive data
- **Data Security** measures include encryption of data both at rest and in motion, physical and logical access controls that prevent unauthorized access etc.
- **Data Protection**, refers to the mechanism of making copies of your data to restore in the event of a loss or corruption.

And what about Checksums and T10 PI?

- Modern transports like FC and SAS have CRC
  - Header and Data integrity on the wire
- PI (Protection information) aka DIF (Data integrity field)
  - Capable of providing end-to-end data protection
  - Data consistency can be validated
- No guarantee against unauthorized data access
  - Data is not encrypted
  - Access doesn't modify protection information
  - Protection only against data modification
- Difference comparable to PGP mail handling
  - 'signing' is equivalent to T10 PI
  - 'encrypting' is equivalent to FC-SP

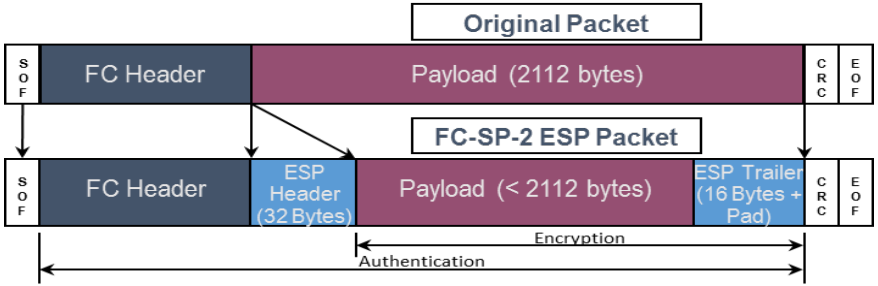
FC-SP-2: What and Why?

- **Why?** : Need to transition SANs from **Authorization and segmentation** based FC security to based security!

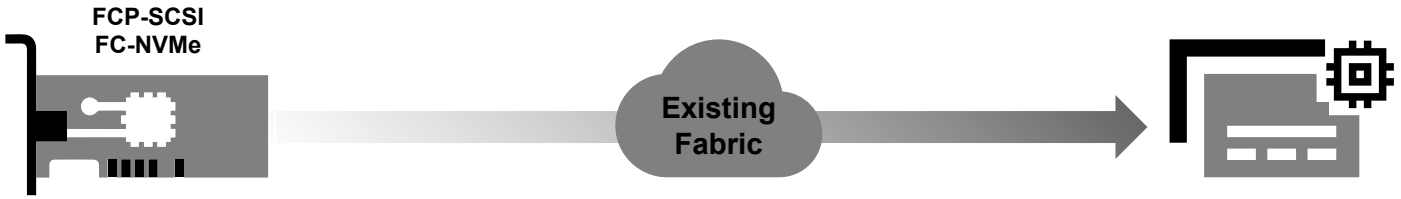
- **What?** FC-SP-2 is an ANSI/INCITS standard (2012) that defines protocols to –
  - **Authenticate** Fibre Channel entities
  - **Setup** session **encryption keys**
  - Negotiate parameters to ensure per **frame integrity and confidentiality**
  - Define and **distribute security policies** over FC

- Designed to protect against several classes of threats

New Generations of FC HBAs provide full offload (Marvell QLogic)



FC-SP-2 Protects FCP and FC-NVMe



“NVMe” Over Fibre Channel
SCSI over Fibre Channel

Non-Volatile Memory “Express”

Concurrent FCP and FC-NVMe	Low Latency
Encrypted in Flight	32GFC and higher speed FC HBAs
Disaggregation for Virtualized DCs	Linux

FC encryption: infrastructure

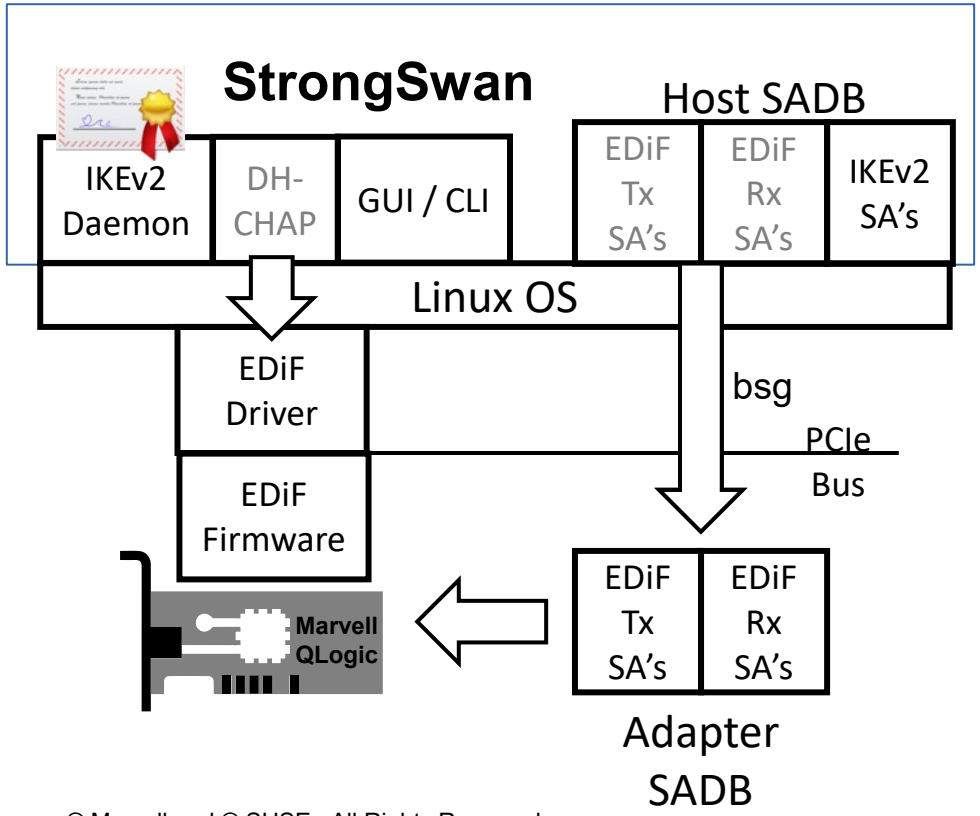
FC-SP-2: The challenges

- Full frame encryption
  - Impossible to run off-card at 32G speeds due to HW bandwidth limitations (PCI Gen3x16 bandwidth 16 GB/s)
- Complex key exchange and key handling
  - implementation within the driver not feasible
  - integration with existing tooling required
- Hard to do it alone
  - much better synergy effects by cooperating between hardware and software vendors
- Marvell-SUSE cooperation to deliver full solution

FC encryption: infrastructure

- FC-encryption is modelled on IPSec encryption
- IPSec encryption provided by Strongswan
- Integration of FC encryption into Strongswan
  - Modifications to Strongswan to handle FC frames
  - Additional module ‘auth-els’ to handle FC-SP-2

FC encryption: strongswan



FC encryption: infrastructure

- FC-SP ELS frames are passed via bsg between kernel and userland
- Strongswan auth-els plugin to process FC-SP ELS frames
- Application-specific bsg frames to control encryption offload
- Linux SCSI netlink messages to react on link changes

FC encryption: configuration

- FC initiator and target configuration unchanged
- FC PRLI blocked as ELS frames are passed to userland via bsg
- Strongswan processes ELS frames
  - Creating Security Association
  - Continues with PRLI
- LUNs will be presented to the initiator

FC encryption: configuration

strongswan status

```
Security Associations (4 up, 0 connecting):
ika_sa 0
--------
210034800d60a101210034800d60a0c7[107]: ESTABLISHED 25 seconds ago, 0.11.96.0[210034800d60a0c7]...0.96.20.0[210034800d60a101]
child_sa 0
----------
210034800d60a101210034800d60a0c7{295}:  INSTALLED, TUNNEL, reqid 107, ESP SPIs: 4aac726a_i 32f9f282_o
210034800d60a101210034800d60a0c7{295}:   0b60..0b60/24[255/0-2551-1] === 60140..60140/24[255/0-2551-1]
ika_sa 1
--------
210034800d60a100210034800d60a0c5[106]: ESTABLISHED 50 seconds ago, 0.29.96.0[210034800d60a0c5]...0.96.22.0[210034800d60a100]

child_sa 1
----------
210034800d60a100210034800d60a0c5{293}:  INSTALLED, TUNNEL, reqid 106, ESP SPIs: 66e7bf64_i a09b8989_o
210034800d60a100210034800d60a0c5{293}:   01d60..01d60/24[255/0-2551-1] === 60160..60160/24[255/0-2551-1]

ika_sa 2
--------
210034800d60a100210034800d60a0c7[104]: ESTABLISHED 104 seconds ago, 0.11.96.0[210034800d60a0c7]...0.96.22.0[210034800d60a100]

child_sa 2
----------
210034800d60a100210034800d60a0c7{289}:  INSTALLED, TUNNEL, reqid 104, ESP SPIs: 54db8c06_i c1661a37_o
210034800d60a100210034800d60a0c7{289}:   0b60..0b60/24[255/0-2551-1] === 60160..60160/24[255/0-2551-1]

[ .. ]
```

FC encryption: configuration

```
# lsscsi
[0:0:0:0]    disk    LIO-ORG  NVDIMM1          4.0   /dev/sdc
[0:0:0:1]    disk    LIO-ORG  NVDIMM2          4.0   /dev/sdf
[0:0:0:2]    disk    LIO-ORG  NVDIMM3          4.0   /dev/sde
[0:0:0:3]    disk    LIO-ORG  NVDIMM4          4.0   /dev/sdd
[0:0:1:0]    disk    LIO-ORG  NVDIMM1          4.0   /dev/sdk
[0:0:1:1]    disk    LIO-ORG  NVDIMM2          4.0   /dev/sdn
[0:0:1:2]    disk    LIO-ORG  NVDIMM3          4.0   /dev/sdm
[0:0:1:3]    disk    LIO-ORG  NVDIMM4          4.0   /dev/sdl
[5:0:0:0]    disk    LIO-ORG  NVDIMM1          4.0   /dev/sdg
[5:0:0:1]    disk    LIO-ORG  NVDIMM2          4.0   /dev/sdj
[5:0:0:2]    disk    LIO-ORG  NVDIMM3          4.0   /dev/sdi
[5:0:0:3]    disk    LIO-ORG  NVDIMM4          4.0   /dev/sdh
[5:0:1:0]    disk    LIO-ORG  NVDIMM1          4.0   /dev/sdo
[5:0:1:1]    disk    LIO-ORG  NVDIMM2          4.0   /dev/sdr
[5:0:1:2]    disk    LIO-ORG  NVDIMM3          4.0   /dev/sdq
[5:0:1:3]    disk    LIO-ORG  NVDIMM4          4.0   /dev/sdp
```

FC encryption: performance

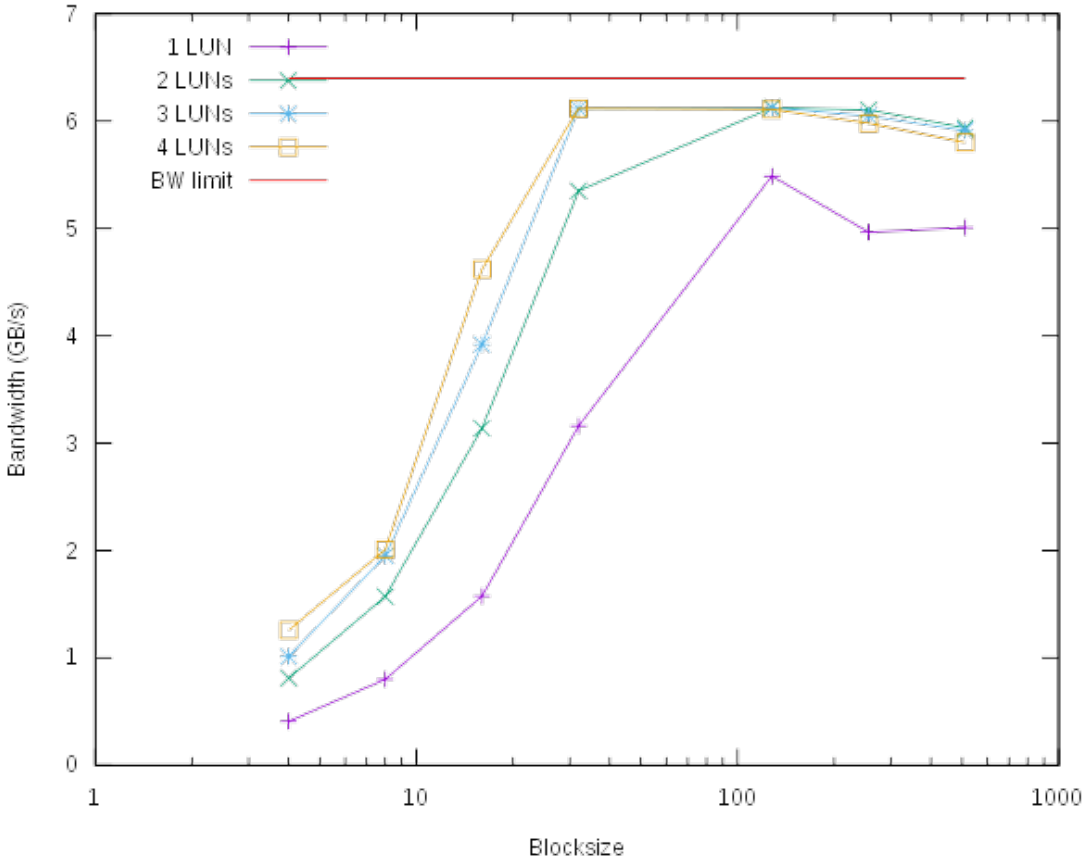
FC encryption: test setup

- Target machine:
  - 48 cores Intel Xeon, 64GB RAM, 512 GB NVDIMM
  - Quad-port Marvell QLogic 32GFC QLE2784 w/ Encryption offload (StorCryption)
- Initiator machine:
  - 40 core/2 socket Intel Xeon, 64 GB RAM
  - Quad-port Marvell QLogic 32GFC QLE2784 w/ Encryption offload (StorCryption)
- Brocade 32GFC switch

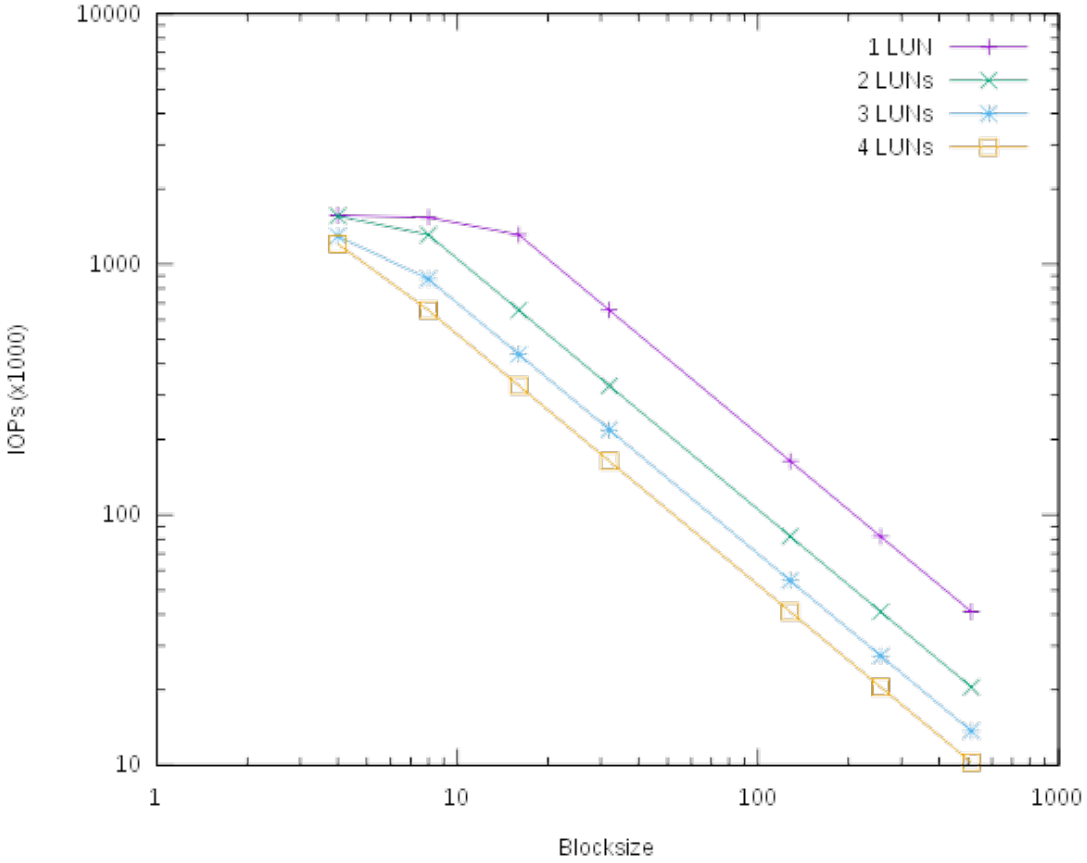
FC encryption: performance

- Linux ‘fio’ tool to test performance
- Bandwidth testing to analyse streaming performance of encryption offload
  - Sequential read and write tests
  - Tests with different I/O block sizes (4k - 512k)
  - Tests with different number of LUNs (1 - 4)

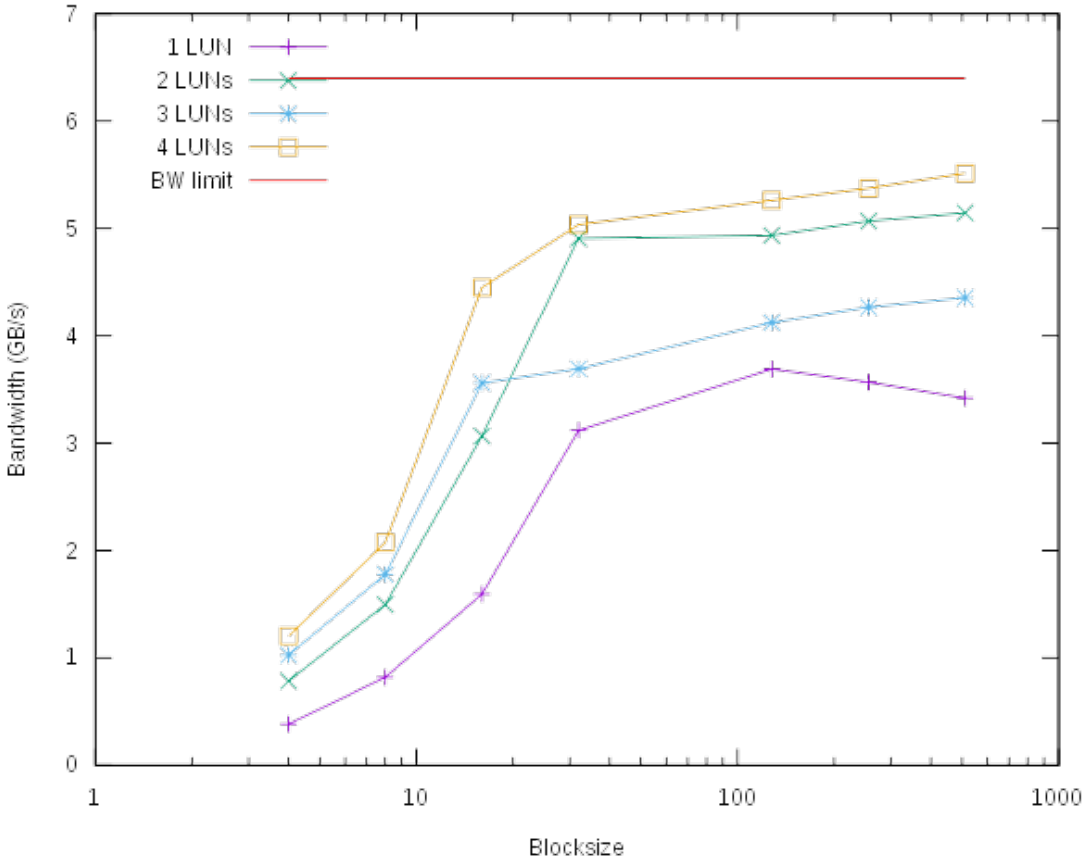
FC encryption: read performance



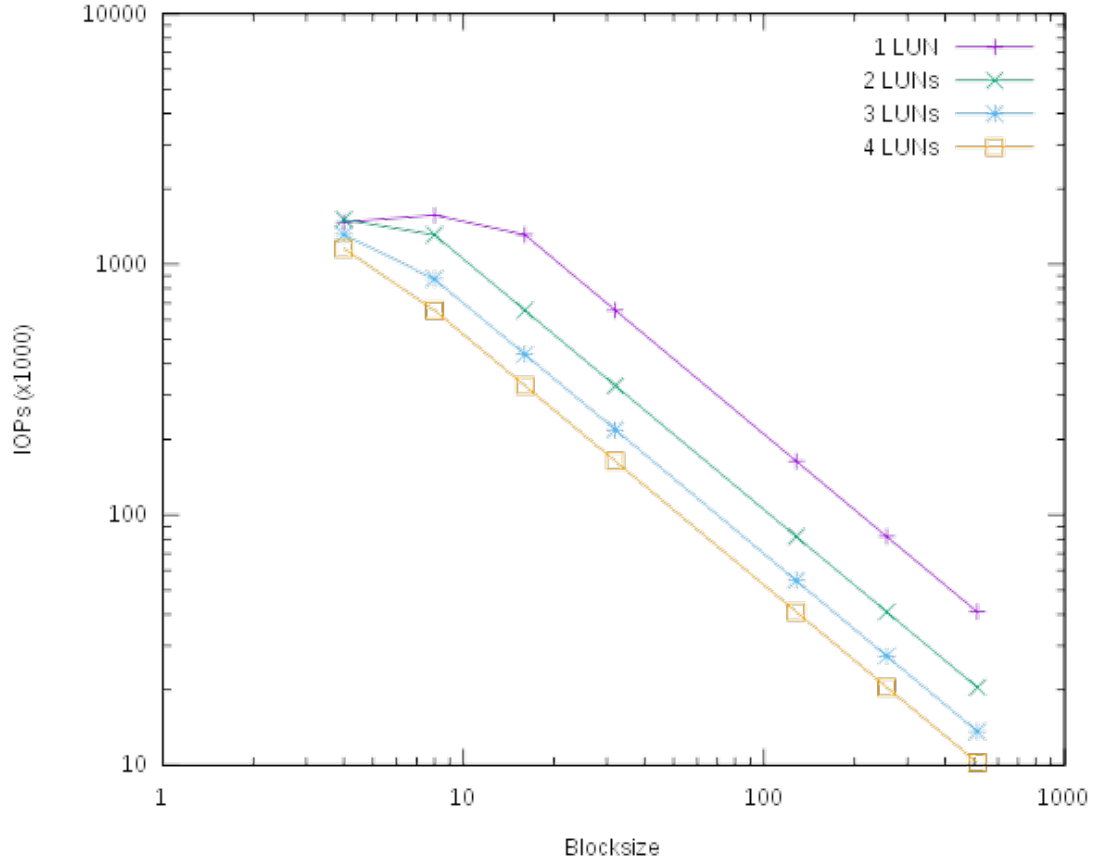
FC encryption: read performance



FC encryption: write performance



FC encryption: write performance



FC encryption: performance results

- Performance is nearing HW limitations:
  - Dual-port 32G FC; nominally 6.4GB/s
  - Target on NV-DIMM with a bandwidth of about 5-6GB/s
  - NV-DIMM write speed noticeably slower than reads
  - Some minor performance impact on larger blocksizes

FC encryption: next steps

Deployment

- Integrating Proof-of-concept code into SLES distribution
- Base enablement with a standard maintenance update
- EdiF-enabled modules for qla2xxx driver and strongswan distributed separately

Upstream work

- *qla2xxx* kernel driver updates:
  - Additional functionality for EDiF (StorCryption)
  - Upstream enablement
- Strongswan update:
  - FC-Frame handling to be upstreamed
  - EdiF specific handline (auth_els) distributed as separate module

Please take a moment
to rate this session.

Your feedback matters to us.