

HPCXXL
2018

IBM Spectrum Scale

Securing Data at Rest and Data in Motion

- Sandeep Patil

Acknowledgement: Felipe Knop ,
Truong Vu, Christof Schmitt, Yong
ZY Zheng, Christopher Maestas



Please note

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

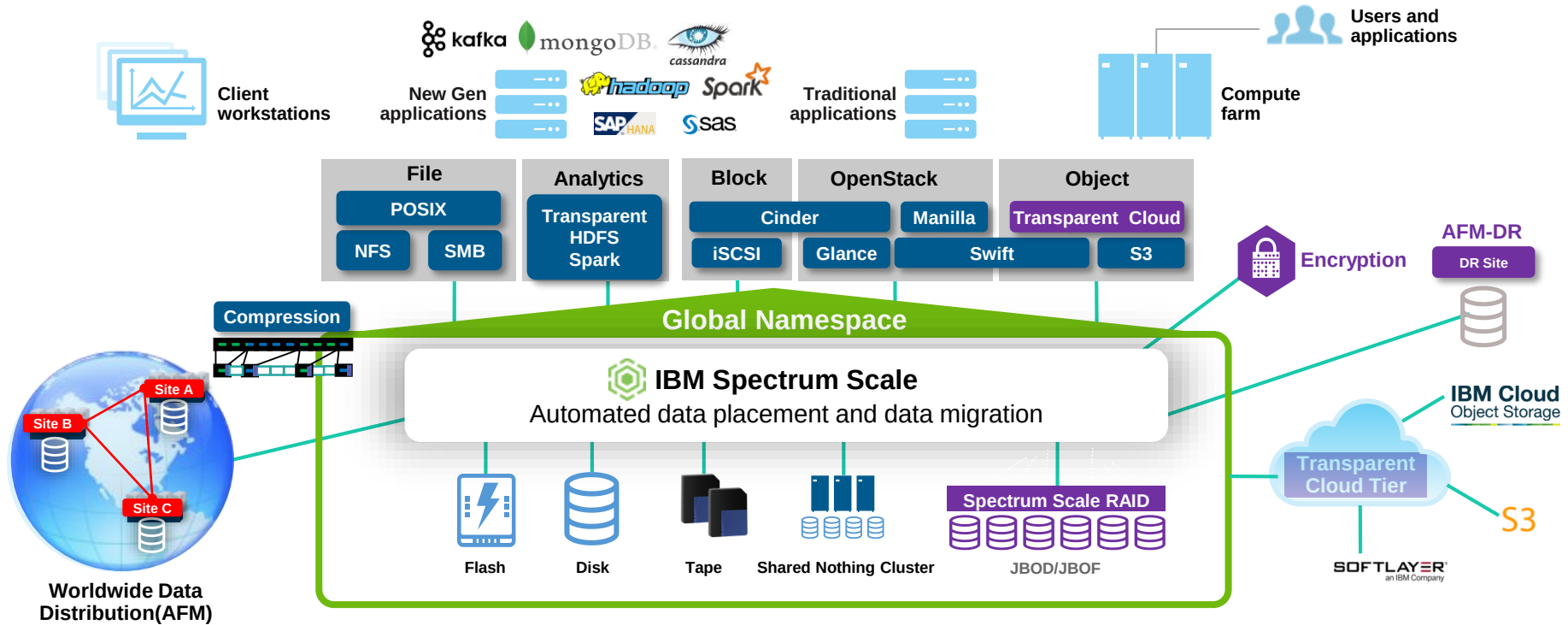
The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features

or functionality described for our products remains at our sole discretion.

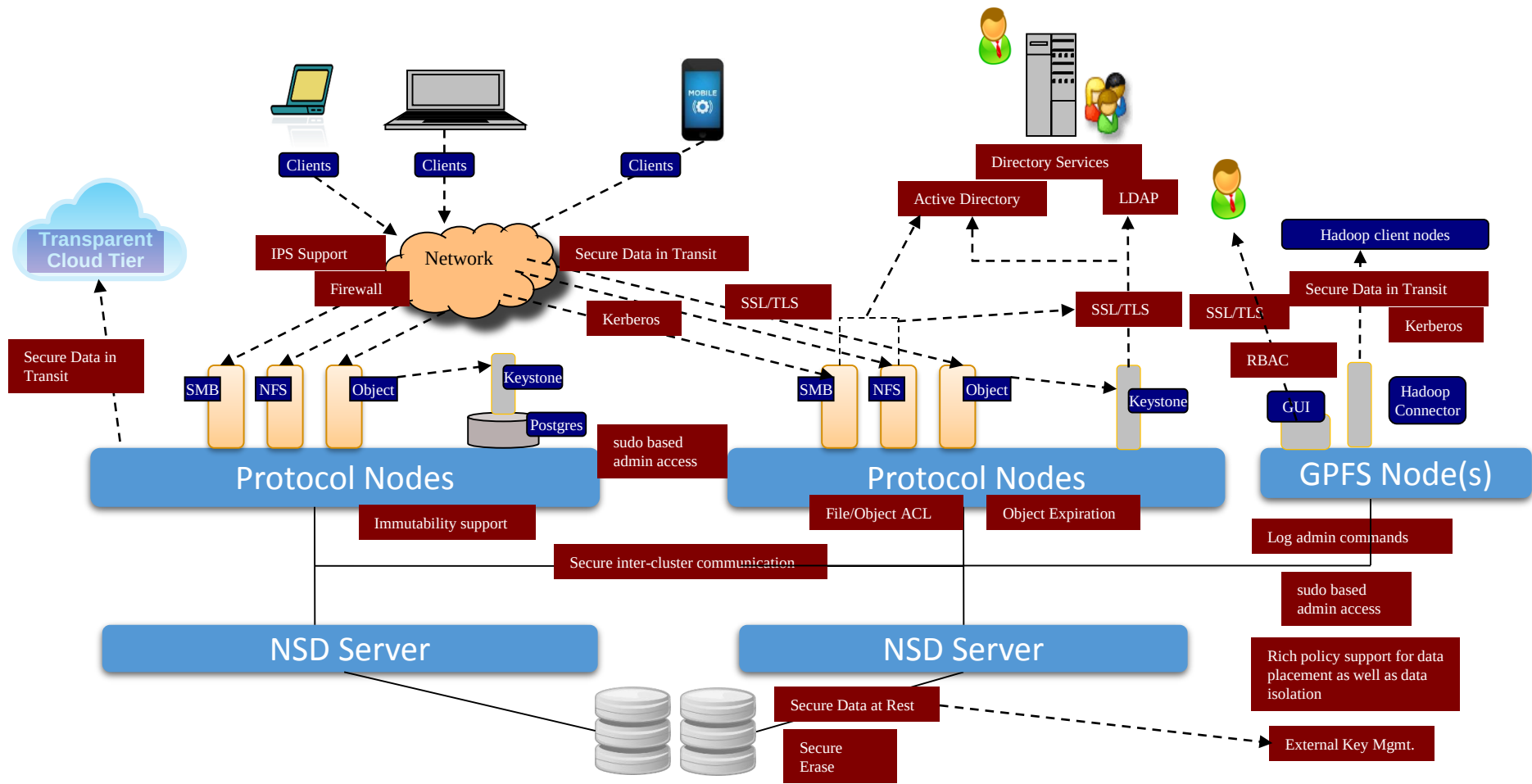
Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

Spectrum Scale: Breath of new features Catering to newer workloads



Consolidate all your unstructured data storage on Spectrum Scale with unlimited and painless scaling of capacity and performance – ENSURING DATA SECURITY !

Spectrum Scale High Level Security Outlook



What we are going to cover today ?

- Secure Data at Rest
- Secure Data in Motion

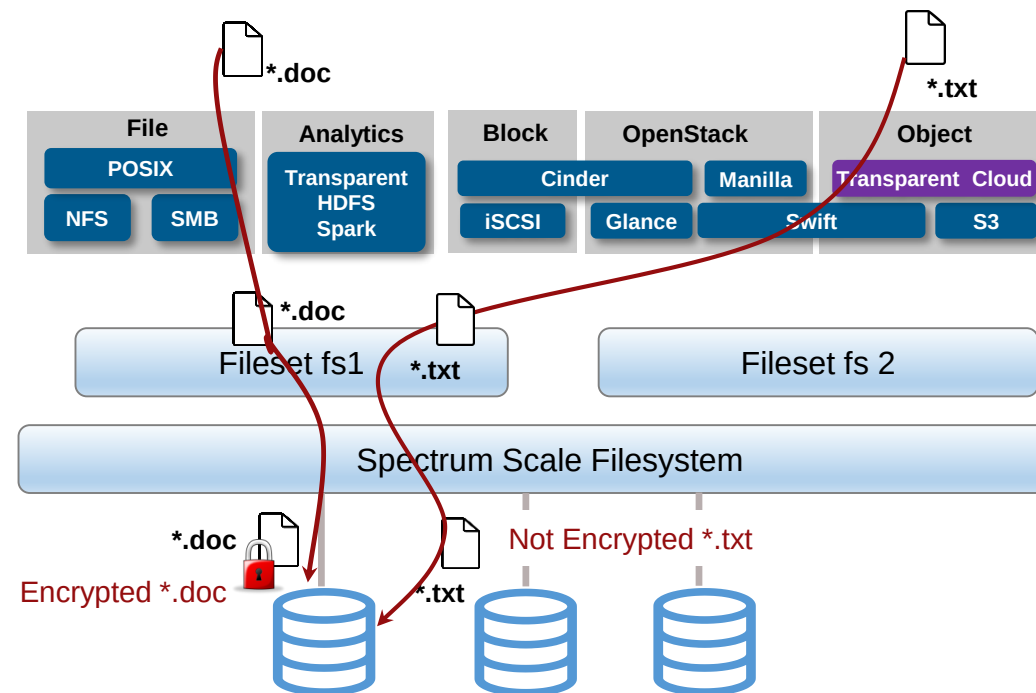
Spectrum Scale Secure Data at Rest : At-A-Glance

Encryption of Data at Rest

- Files are encrypted before they are stored on disk
- Master Keys are never written to disk
- No data leakage in case disks are stolen or improperly decommissioned

Secure Deletion

- Ability to destroy files with no data remanence
- No “digital shredding” secure delete is cryptographic operator



NIST & FIPS

- The encryption algorithms that are used for file encryption are all compliant with NIST Special Publication 800-131A.
- Allows cluster to be configured in FIPS mode

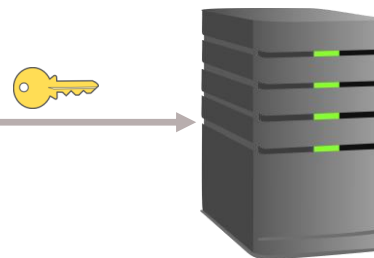
Encryption policy rules:

- which files are to be encrypted,
- with which algorithm,
- using which MEKs.

Example encryption policy rules

```
RULE 'myEncRule1' ENCRYPTION 'E1' IS  
ALGO 'DEFAULTNISTSP800131A'  
KEYS('1:RKM_1', '2:RKM_2')
```

```
RULE 'Encrypt files with extension doc with rule E1'  
SET ENCRYPTION 'E1'  
FOR FILESET('fs1')  
WHERE NAME LIKE '%.doc'
```



External Key Manager Server
(IBM SKLM or Vormetric DSM Key Server)

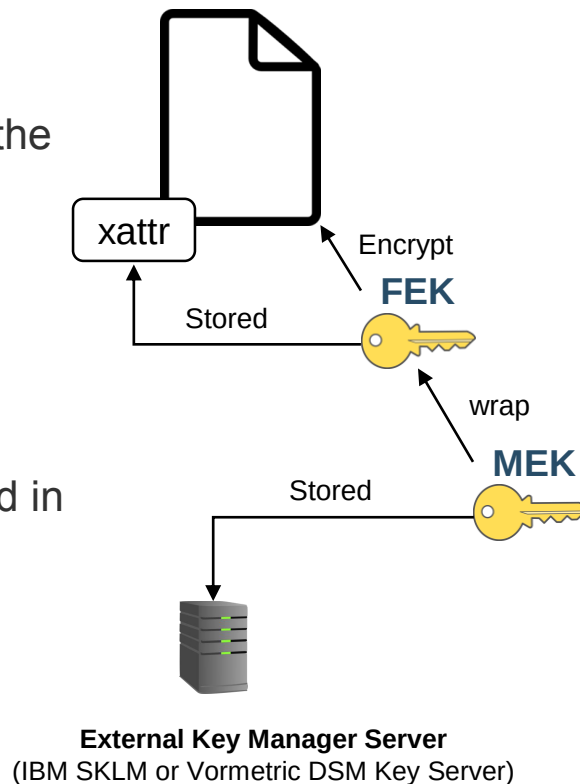
Spectrum Scale Secure Data At Rest- Key-based encryption

Master Encryption Key (MEK)

- Used to encrypt file encryption keys
- Stored in Remote Key Management (RKM) Servers
- MEK's have a unique key name that combines the name of the key and the RKM server where it resides

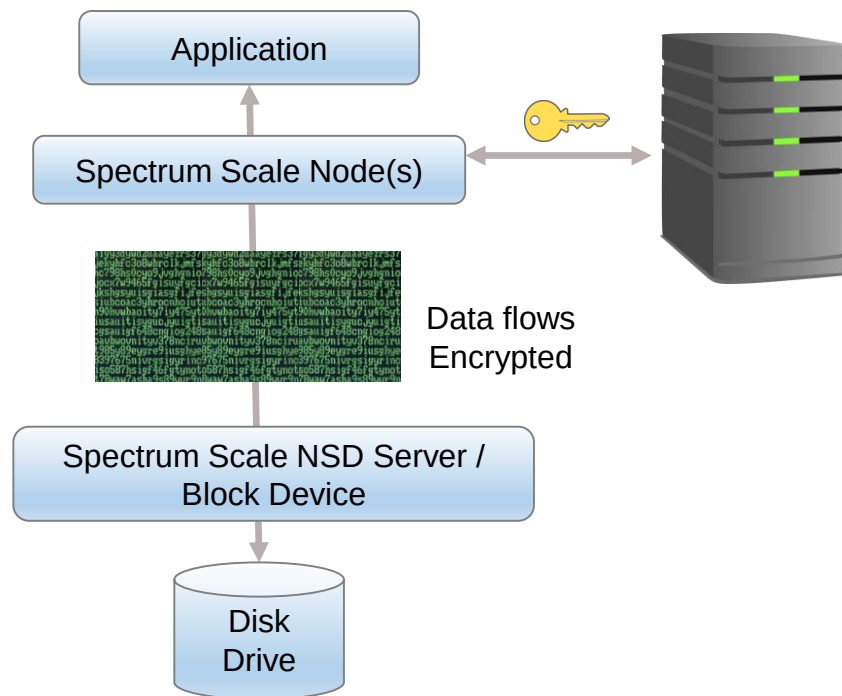
File Encryption Key (FEK)

- Used to encrypt sectors of an individual file
- Unique key randomly generated
- Encrypted (or “wrapped”) with one or more MEK's and stored in the extended attribute on filesystem.
- FEK must have access to MEK to be decoded
- FEK can be re-wrapped to new MEK(s) in the case of a compromised key



Spectrum Scale Secure Data At Rest: Native Filesystem encryption

- Files encrypted before I/O submission
- Encryption takes place on the node(s) from which the user drives the I/O
- File content travels encrypted to the NSD server
- MEKs can be accessed by nodes that have appropriate RKM credentials
- Nodes that cannot access keys cannot access files, irrespective of file permissions
- Granularity is per file or per fileset, as determined by encryption policies



How to Enable File System Encryption ?

- **Encryption Policies**

- Manage how files are encrypted and includes the following:
 - Which files are to be encrypted
 - Which algorithm is to be used for encryption
 - Which MEK (or MEK's) are to be used to wrap the FEK of a file
- The **mmchpolicy** command is used to configure encryption and is applied at file creation time.
- When a file is created, encryption rules are executed. If the file matches at least one SET ENCRYPTION rule, an FEK is generated and used to encrypt the contents of the file.
- The FEK is then wrapped using the stated encryption rule using the MEK and stored in the file's extended attribute.

Example

Example encryption policy rules

RULE 'myEncRule1' ENCRYPTION 'E1' IS

ALGO '**DEFAULTNISTSP800131A**'

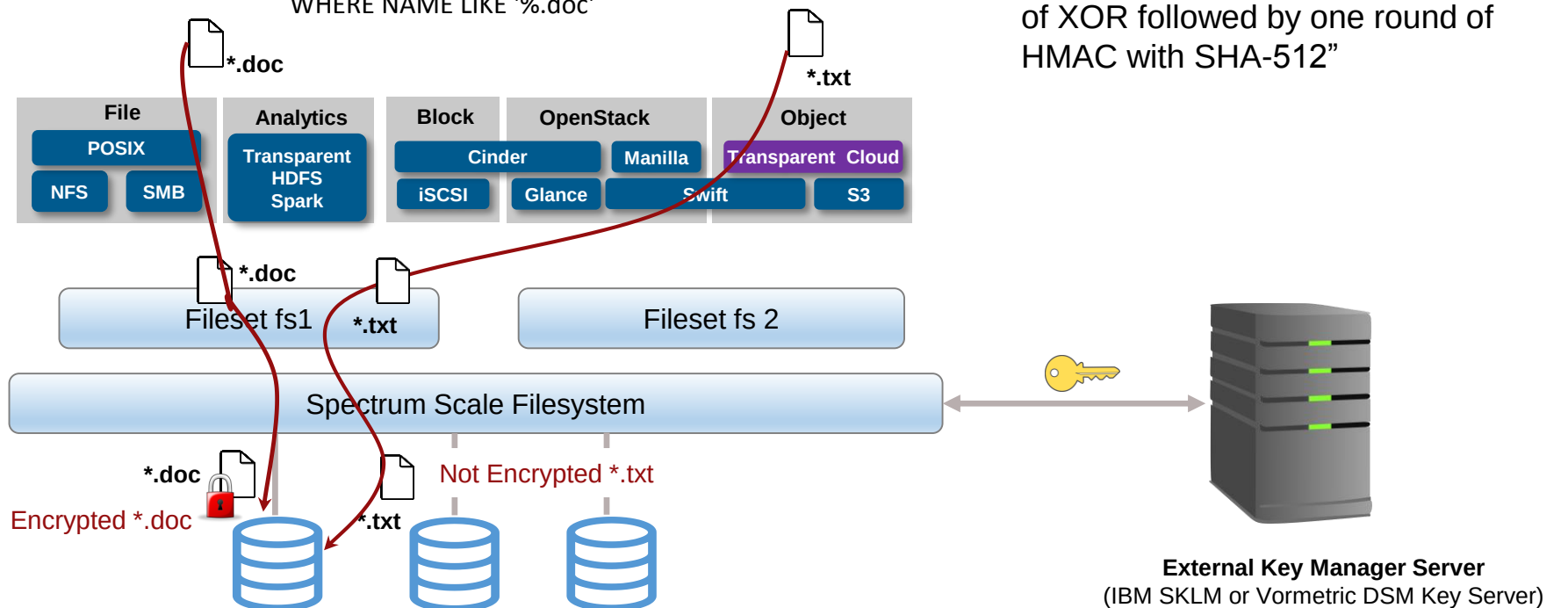
KEYS('1:RKM_1', '2:RKM_2')

RULE 'Encrypt files with extension doc with rule E1'

SET ENCRYPTION 'E1'

FOR FILESET('fs1')

WHERE NAME LIKE '%.doc'



FAQ – Spectrum Scale Filesystem Encryption

1. Should all nodes have access to the Remote Key Manager?

Yes , all nodes that may access the FS, including nodes with management roles like NSD servers, POSIX clients FS managers, etc

2. Does data travel in encrypted form from NSD servers to NSD clients (intra-cluster) when Filesystem is configured for encryption ?

Yes, but only the 'data' and not the intra-cluster RPC.

3. Can I have selective encryption for a given set of files ?

Yes, as far as you can write policies to determine those files.

4. Can I encrypt existing set of files which were present before the encryption was enabled ?

No. You need to copy the files into newly-created encrypted counterparts, possibly using a migration policy.

5. Where are the Encrypted FEK stored ?

Encrypted FEK are stored in the 'gpfs.Encryption' extended attribute of the file.

6. How do I find out if a given file is Encrypted ?

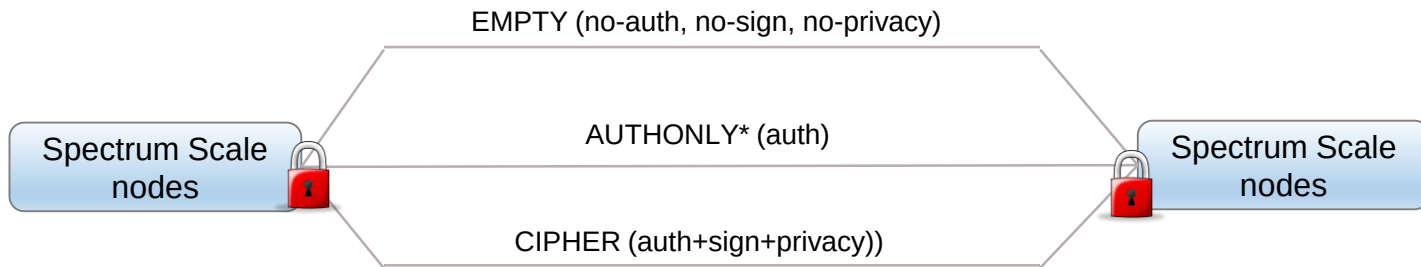
Run `'mmlsattr -n gpfs.Encryption /gpfs1/file-name'`

7. How do I find out if the Filesystem is configured for Encryption?

Spectrum Scale : Secure Data at Motion

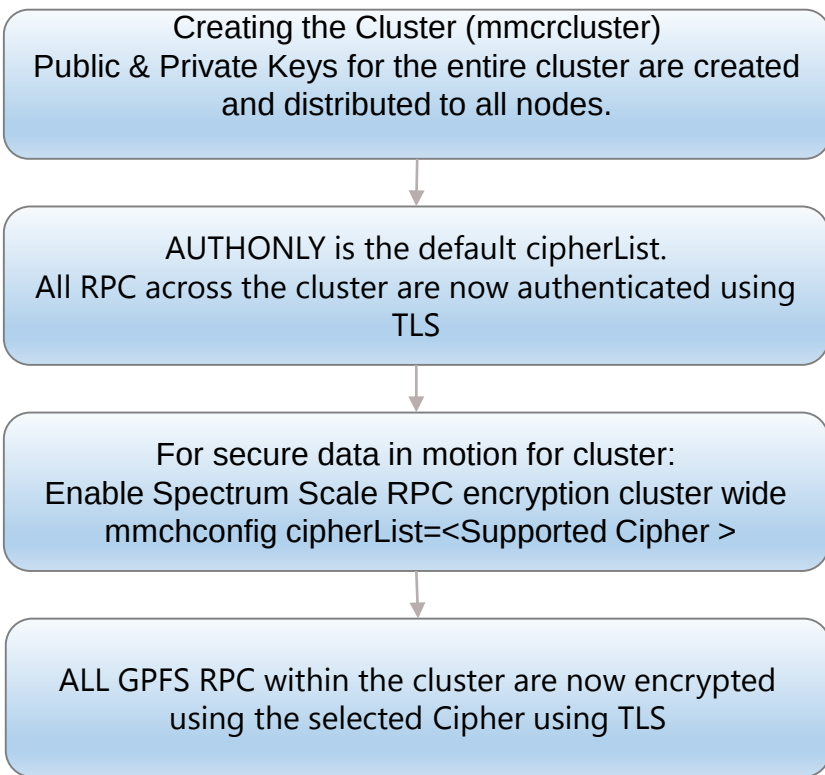
- Data in transit, also referred as Data in Motion or Data in Flight, is data that is being accessed over a network (internal or external) and can therefore be intercepted by malicious users on the network.
- Based on your business needs or on the sensitivity of your data that is being accessed over the network, one needs to **protect it by encryption over the wire**.

Spectrum Scale Secure Cluster Communication



AUTHONLY* perform TLS authentication, but then all RPC traffic goes in the clear.

Configuration Flow for Secure Data in Motion Between Nodes Within a Cluster



Notes:

- Use mmauth command to generate new set of Keys for the cluster.
- The keys are located in `/var/mmfs/ssl/`
- The authentication , integrity check and encryption is based on TLS mechanism.
- Expiration of the keys can be monitored by the admins using openssl commands.
- Supported Ciphers
 - AES128-SHA
 - AES128-SHA256
 - AES256-SHA
 - AES256-SHA256

Configuration Flow for Secure Data in Motion Between Cluster

CLUSTER 1

Generate Keys : `mmauth genkey new`
Enforce Encryption:
`mmauth update . -I AES128-SHA256`

Public key of cluster 1 given to admin of
cluster 2
`/var/mmfs/ssl/id_rsa.pub`

Add the Remote Cluster that will access the filesystem
and its Public Key
`mmauth add cluster2 -k cluster2_id_rsa.pub`

Grant the remote cluster secure access to a
filesystem
`mmauth grant cluster2 -f gpfs0`

CLUSTER 2 (Remote)

Generate Keys : `mmauth genkey new`
Enforce Encryption:
`mmauth update . -I AES128-SHA256`

Public key of cluster 2 given to admin of
cluster 1
`/var/mmfs/ssl/id_rsa.pub`

Add the cluster to be accessed along with its key and
nodes used to access.
`mmremotecluster add cluster1 -n node1,node2,node3 -k
cluster1_id_rsa.pub`

Add the remote filesystem that will be accessed by the
cluster
`mmremotefs add mygpfs -f gpfs0 -C cluster1 -T /mygpfs`
Followed by
`mmm mount mygpfs`



FAQ - Secure Data in Motion For Cluster Communication

1. What are the supported Ciphers Type by Spectrum Scale for cluster communication?

'mmauth show ciphers' list all the support Ciphers.

2. How do I determine which encryption Algorithm is being used for secure cluster communication ?

For intra-cluster communication:

It is the value set via *'mmchconfig CipherList'* and can be viewed via *'mmlsconfig cipherList'* or even via *'mmauth show all'* (look for "Cipher list" the local cluster entry)

For inter-cluster communication:

'mmauth show all' shows the encryption algorithm being used with remote cluster

3. How to Change the Encryption Algo being used for cluster communication ?

For intra-cluster communication:

'mmchconfig cipherlist=security_mode'

For inter-cluster communication:

Update the supported Cipher type that you want to mandate the the remote cluster to use for communication . Setting takes effect for newer cnpnnections.

Example: Mandate remote cluster (cluster 2) with *AES128-SHA for communication* run *'mmauth update cluster2 -I AES128-SHA'* on local cluster.

4. How do I change the cluster certificates of my cluster ?

Use *'mmauth'* command . Check Knowledge Center for details.

FAQ - Secure Data in Motion For Cluster Communication

5. How do I check if my certificates are going to expire ?

Use openssl commands to check your cluster certificates located in /var/mmfs/ssl
'`openssl x509 -in id_rsa_committed.cert -noout -dates`'

6. Are default certificate for a cluster created when cluster is created ?

Yes, from IBM Spectrum Scale V4.2 or later *mmcrcluster* creates the certificates for the cluster and are propagated to all the nodes. The nodes make use of these certificate for secure communication which is based on TLS with AUTHONLY as the default security mode.

7. For inter cluster communication, can I mandate specific Ciphers to communicate with other clusters ?

Yes. You can choose what kind of secure communication you want to have with a given cluster. Need to use *mmauth* command. Check Knowledge Center for examples.

8. If I want to use NIST complaint encryption algorithm , which Algorithms should I set to the CipherList ?

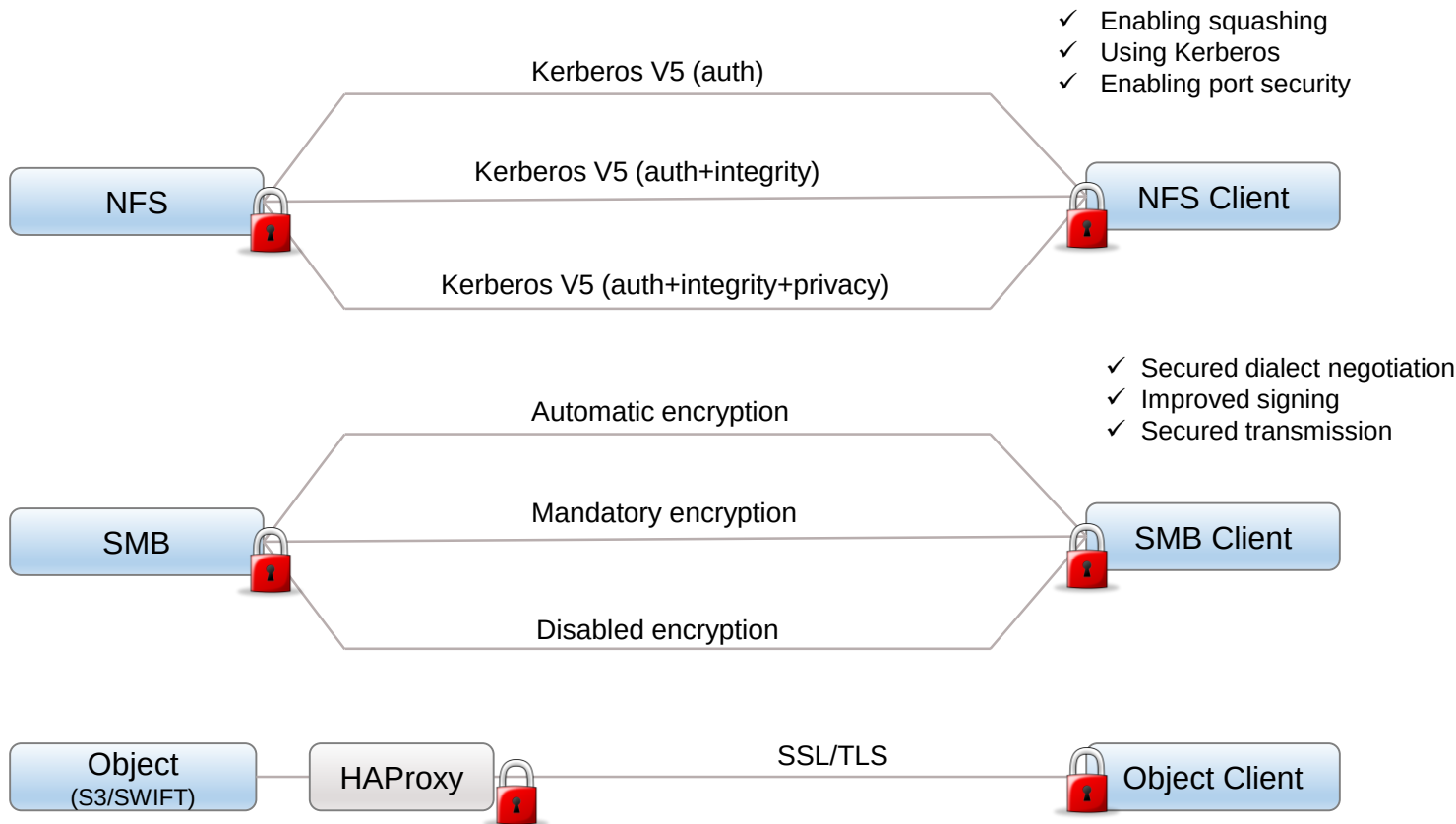
'*mmauth show ciphers*', should show you the list which includes NIST complaint encryption algorithms.

9. What is the significance of mmchconfig nistCompliance=SP800-131A ?

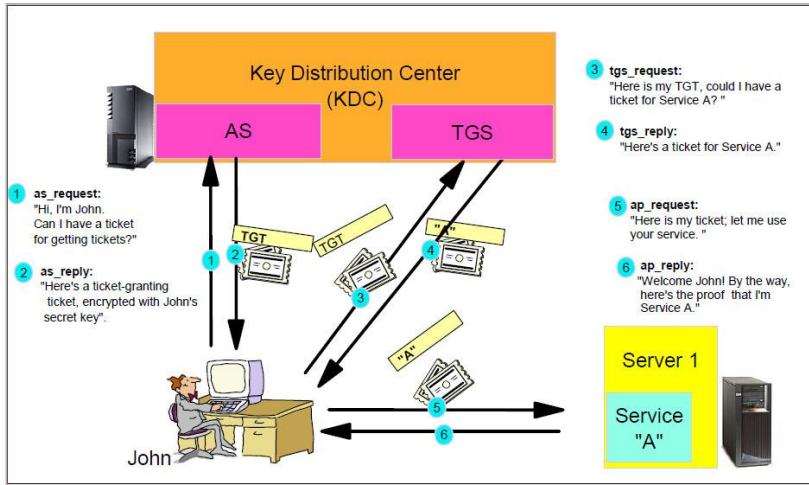
Setting *nistCompliance* governs what values to 'CipherList' can be set/reset using *mmchconfig* command. When set to SP800-131A only NIST complaint algorithms are allowed to be set.

Spectrum Scale : Secure Data at Motion for Protocols

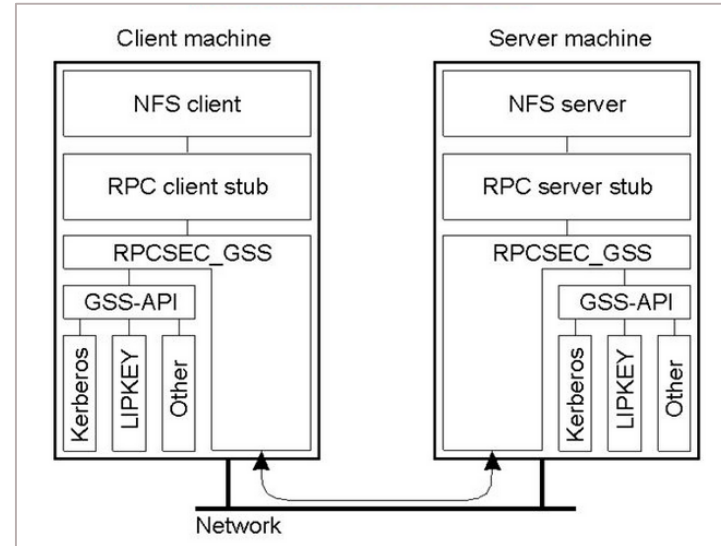
Secure access of Spectrum Scale File Interfaces



Secure Data at Flight for NFS, SMB based on Kerberos



SOURCE: <https://www.ibm.com/developerworks/ibmi/library/i-ss0/index.html>



Source: <http://csis.pace.edu/~marchese/CS865/Lectures/Chap11/Chapter11.htm>

- NFS , SMB (Samba) is just another service to Kerberos.
- NFS makes use of Kerberos via GSS-API to provide authentication, integrity check and per-message encryption.
- Enabling per message encryption for NFS / SMB shares ensures secure data in flight for NFS and SMB access.

Configuration– Kerberized NFS

NFS Configuration Steps

- Ensure Prerequisites for configuring Kerberos based NFS access are in place.
 - NFS server configuration file changes to reflect Kerberos realm names
 - NFS client configuration changes to reflect Kerberos realm name and start of NFS secure Linux services
 - Keytab file creation in case of LDAP+MIT KDC and transfer to protocol nodes
 - Configuring appropriate Kerberos auth using mmuserauth based on backend directory server.
 - Detail Prerequisite mention in Knowledge Center -
https://www.ibm.com/support/knowledgecenter/en/STXKQY_5.0.1/com.ibm.spectrum.scale.v5r01.doc/b1ladm_prereqforkerbnfsaccess.htm
- **'krb5p' SECTYPE Clientoptions need to be used with *mmnfs export add | change* for NFS data encryption for that NFS export**

mmnfs export add /ibm/gpfs0/fset1 -client

"*(Access_Type=RW,Squash=no_root_squash,SecType=krb5p)"

On RHEL Linux Client: **mount -t nfs -o vers=4,sec=krb5p**
ckcluster.ad.com:/ibm/gpfs0/fset1 /mnt/4k5p -vvvv

Secure Data in Flight for SMB

- Spectrum Scale **supports encryption** for the **SMB3** protocol
- Only requirement is to use a **client version that supports SMB3** (e.g. Windows 8, Windows Server 2012 or newer)
- After successful authentication, **encryption secrets** are **derived** from the **exchange information** and can be used to encrypt protocol traffic.
- The encryption algorithm also guarantees integrity, so it **equivalent to encryption and signing**.
- The **complete traffic** for a SMB connection can be **encrypted** or only the **traffic to certain SMB shares**.
- Encryption leverages CPU **crypto hardware acceleration**

Configuration– Secure Data in Flight for SMB

SMB Configuration Steps

- **‘smb encrypt’** option need to be used with **mmsmb export add | change** for SMB data encryption (can be specified per SMB share or globally)
- **Values:**
 - auto - SMB encryption is offered, but not enforced.
 - mandatory -SMB encryption is required
 - disabled - SMB encryption can not be negotiated.

Example:

- `mmsmb export add myExport "/ibm/gpfs0/myFolder" --option "smb encrypt = mandatory"`
- Note: SMB share must be mounted using Netbiois name).

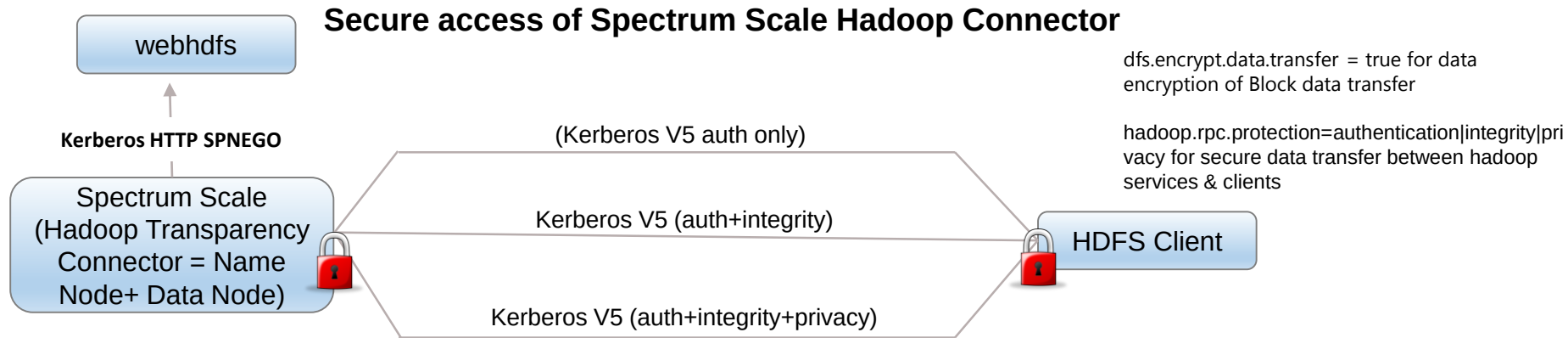
Network Trace : Show Secure Data in Flight (SMB)

The best illustration for secure data in rest is a network trace:

- In this example we have the **complete SMB connection encrypted** (smb encrypt = mandatory in the global config). You see here that the connection is established, features are negotiated and authentication is done through the SESSION_SETUP exchanges. Everything following that is **encrypted**:

7	2018-05-02 08:45:03.719530	9.11.102.184	9.11.102.234	SMB2	168 Negotiate Protocol Request
9	2018-05-02 08:45:03.734505	9.11.102.234	9.11.102.184	SMB2	284 Negotiate Protocol Response
12	2018-05-02 08:45:03.737196	9.11.102.184	9.11.102.234	SMB2	222 Session Setup Request, NTLMSSP_NEGOTIATE
13	2018-05-02 08:45:03.738757	9.11.102.234	9.11.102.184	SMB2	411 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
14	2018-05-02 08:45:03.739290	9.11.102.184	9.11.102.234	SMB2	755 Session Setup Request, NTLMSSP_AUTH, User: EXAMPLE\cschmit
15	2018-05-02 08:45:03.771930	9.11.102.234	9.11.102.184	SMB2	161 Session Setup Response
16	2018-05-02 08:45:03.772483	9.11.102.184	9.11.102.234	SMB2	280 Encrypted SMB3
17	2018-05-02 08:45:03.803795	9.11.102.234	9.11.102.184	SMB2	192 Encrypted SMB3
18	2018-05-02 08:45:03.804084	9.11.102.184	9.11.102.234	SMB2	266 Encrypted SMB3
19	2018-05-02 08:45:03.804522	9.11.102.234	9.11.102.184	SMB2	248 Encrypted SMB3
20	2018-05-02 08:45:03.804736	9.11.102.184	9.11.102.234	SMB2	360 Encrypted SMB3
21	2018-05-02 08:45:03.805750	9.11.102.234	9.11.102.184	SMB2	296 Encrypted SMB3

Spectrum Scale : Secure Data at Motion



Between Hadoop Client and Services (NameNode)

- Uses Java SASL (Simple Authentication & Security Layer) API
- On both set of nodes Set `hadoop.rpc.protection` in `core-site.xml` to:
 - authentication (default)
 - integrity (includes authentication)
 - privacy (includes integrity + authentication)

Between HDFS Client and DataNode

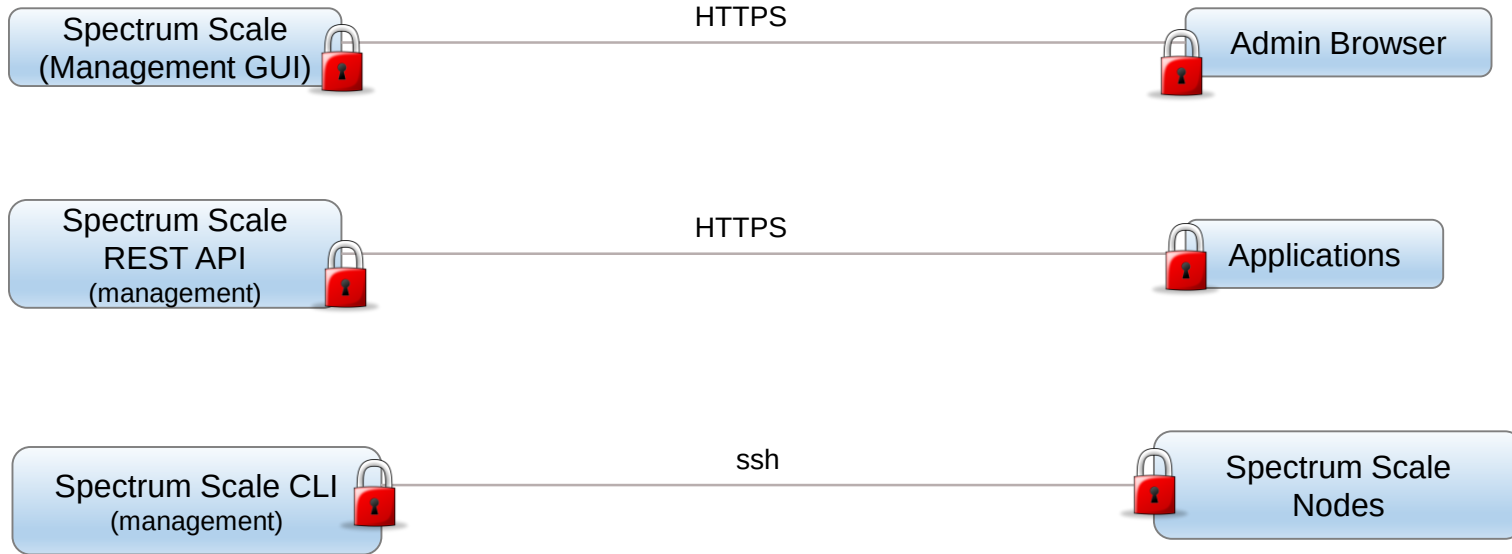
- On both set of nodes set following in `hdfs-site.xml`
 - `dfs.encrypt.data.transfer = true`
 - `dfs.encrypt.data.transfer.algorithm = 3des` (default) OR `rc4`

To use AES:

- `dfs.encrypt.data.transfer.cipher.suites = AES/CTR/NoPadding`
- `dfs.encrypt.data.transfer.cipher.key.bitlength = 128` (default) OR 192 OR 256

Spectrum Scale : Secure Management

Secure access of Spectrum Scale Management



Administration of Spectrum Scale requires Remote Shell and Remote Copy (SSH and scp are default and recommended)

IBM Spectrum Scale : Security Redpaper & Blogs

- Redpaper (refresh) – Released Sept 2018
<http://www.redbooks.ibm.com/abstracts/redp5426.html?Open>
- Security Blogs by Developers: <https://developer.ibm.com/storage>
- Enhanced Knowledge Center with all details.
- Spectrum Scale Immutability whitepaper: <http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP102620>
- For Kerberized NFS with LDAP-Kerberized authentication scheme:
<https://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/TD106395>
- For Kerberized NFS with AD-Kerberized authentication scheme:
<https://crk0acr0a.wordpress.com/2016/07/19/ibm-spectrum-scale-kerberized-nfs-with-ad-rfc2307/>



HPCXXL 2018

Thank You !



Ciphers Supported by Spectrum Scale tscomm layer

`c10c1apv7:~ # mmauth show ciphers`

Supported ciphers for `nistCompliance=SP800-131A`:

AES128-GCM-SHA256

AES128-SHA

AES128-SHA256

AES256-GCM-SHA384

AES256-SHA

AES256-SHA256

DES-CBC3-SHA

Supported ciphers for `nistCompliance=off`:

AES128-SHA

AES256-SHA

DES-CBC-SHA

DES-CBC3-SHA

EXP-RC2-CBC-MD5

EXP-RC4-MD5

RC4-MD5

RC4-SHA

Supported ciphers for both environments:

AES128-SHA

AES256-SHA

DES-CBC3-SHA

For NIST Compliance mode use the following:

`mmchconfig nistCompliance=SP800-131A`

- The `nistCompliance` variable applies to security transport (tscomm security, key retrieval) only, not to encryption, which always uses NIST-compliant mechanisms.
- SP800-131A Specifies that security transport is to follow the NIST SP800-131A recommendations. For clusters at the GPFS 4.1 level or higher, this is the default.

Secure erase : Overview

- **Cannot be achieved with standard methods:**
unlink() leaves data on disk,
overwriting is cumbersome and may not work (e.g. SSD)
- **Secure Cryptographic Erase**
When MEK is deleted, encrypted FEK is no longer retrievable Hence, file cannot be decrypted
Regardless of cached copies, snapshots, backups, ...
- **Two-step operation**
 - Files are deleted with standard file system operations (e.g. rm, unlink...)
 - Secure deletion committed with key management operation
 - Registration of new MEK
 - Re-encryption of FEKs that “need to stay”
 - Deletion of old MEK

Secure erase : High Level Process

- At a high level, the steps for secure deletion are (assuming the files are already encrypted):
 - Remove the file using commands like rm / unlink
 - Create a new (master) key
 - Change the existing policy to "point" to the new key
 - Run a rewrap policy (using mmapplypolicy) to rewrap all files which are to be **kept**, making them use the new key --> that's may be an expensive operation depending on the number of files that need to be traversed.
https://www.ibm.com/support/knowledgecenter/STXKQY_5.0.2/com.ibm.spectrum.scale.v5r02.doc/bl1adv_encryptionpolicyrules.htm
 - Remove the old key from the server
- After the last step, the file is considered secure-deleted. It is the last step that ensures that nobody will be able to decrypt the file, even if someone could get access to the raw content of the disk.

How to Change the Encryption Algorithm that you want to use for Spectrum Scale RPC Communication

- For secure data in motion within the Cluster
 - **mmchconfig cipherList=<cipher>** works to set the cipher for communications within the cluster.
- **For remote cluster communication**
- Using multiple security levels for remote access and changing the Cipher types
 - In this example, cluster2 is accessing file systems that are owned by cluster1 by using a cipherList of AUTHONLY, but the administrator of cluster1 decides to require a more secure cipherList. The administrator of cluster1 issues this command:

mmauth update cluster2 -l AES128-SHA

Existing connections is upgraded from AUTHONLY to AES128-SHA.

Network Trace : Show Secure Data in Flight (SMB) at Share Level

The best illustration for secure data in rest is a network trace:

- Here is an example where traffic to one share is encrypted (smb encrypt = mandatory on one SMB share). The requests on top are visible in the trace. Only everything that relates to the smbencrypt share is encrypted. For encrypted traffic, there is a TRANSFORM header that only specifies that the following data is AES-128-CCM encrypted:

15	2018-05-02 08:41:28.373054	9.11.102.234	9.11.102.184	SMB2	133 Ioctl Response, Error: STATUS_PENDING
16	2018-05-02 08:41:28.373129	9.11.102.234	9.11.102.184	SRVSVC	500 NetShareEnumAll response
18	2018-05-02 08:41:28.373309	9.11.102.184	9.11.102.234	SMB2	148 Close Request File: srvsvc
19	2018-05-02 08:41:28.373620	9.11.102.234	9.11.102.184	SMB2	184 Close Response
21	2018-05-02 08:41:30.737160	9.11.102.184	9.11.102.234	SMB2	278 Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \sandrattler-vm1.tuc.stglabs.ibm.com\smbencrypt
22	2018-05-02 08:41:30.737432	9.11.102.234	9.11.102.184	SMB2	133 Ioctl Response, Error: STATUS_NOT_FOUND
23	2018-05-02 08:41:30.737899	9.11.102.184	9.11.102.234	SMB2	228 Tree Connect Request Tree: \\sandrattler-vm1.tuc.stglabs.ibm.com\smbencrypt
24	2018-05-02 08:41:30.739512	9.11.102.234	9.11.102.184	SMB2	140 Tree Connect Response
25	2018-05-02 08:41:30.739659	9.11.102.184	9.11.102.234	SMB2	266 Encrypted SMB3
26	2018-05-02 08:41:30.741745	9.11.102.234	9.11.102.184	SMB2	248 Encrypted SMB3
27	2018-05-02 08:41:30.743848	9.11.102.184	9.11.102.234	SMB2	288 Encrypted SMB3
28	2018-05-02 08:41:30.745026	9.11.102.234	9.11.102.184	SMB2	352 Encrypted SMB3
29	2018-05-02 08:41:30.745985	9.11.102.184	9.11.102.234	SMB2	360 Encrypted SMB3
30	2018-05-02 08:41:30.746363	9.11.102.234	9.11.102.184	SMB2	185 Encrypted SMB3
31	2018-05-02 08:41:30.746451	9.11.102.184	9.11.102.234	SMB2	208 Encrypted SMB3

Frame 25: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits)

Linux cooked capture

Internet Protocol Version 4, Src: 9.11.102.184, Dst: 9.11.102.234

Transmission Control Protocol, Src Port: 57573 (57573), Dst Port: microsoft-ds (445), Seq: 1710, Ack: 1527, Len: 210

NetBIOS Session Service

SMB2 (Server Message Block Protocol version 2)

SMB2 Transform Header

- Server Component: SMB2_TRANSFORM
- Signature: f6743e477ebcc0ecc55b1df3eee3dea3
- Nonce: 57010000000000005dd7239100000000
- Message size: 154
- Reserved: 0000
- Encryption ALG: 0x0001, SMB2_ENCRYPTION_AES128_CCM
- Session Id: 0x000000009123d75d

Encrypted SMB3 data

Data: 043e0a9833b06db9948192ad66cd81176940b1172e495564...

Security Requirement Vs Spectrum Scale Security Capabilities

Key Security requirement	Spectrum Scale Capability
Secure Data at Rest	✓
Secure Data in Transit	✓
Authentication	✓
Authorization	✓
Secure Administration	✓
Immutability	✓
Firewall	✓
Hadoop Security	✓
Cloud Tiering Security	✓
Audit Logging	✓
Anti Virus	✓ Basic Covered

High Level Flow for Kerberos

2. AS verifies user's access right in database, create ticket-granting ticket and session key. Results are encrypted using key derived from user's password.

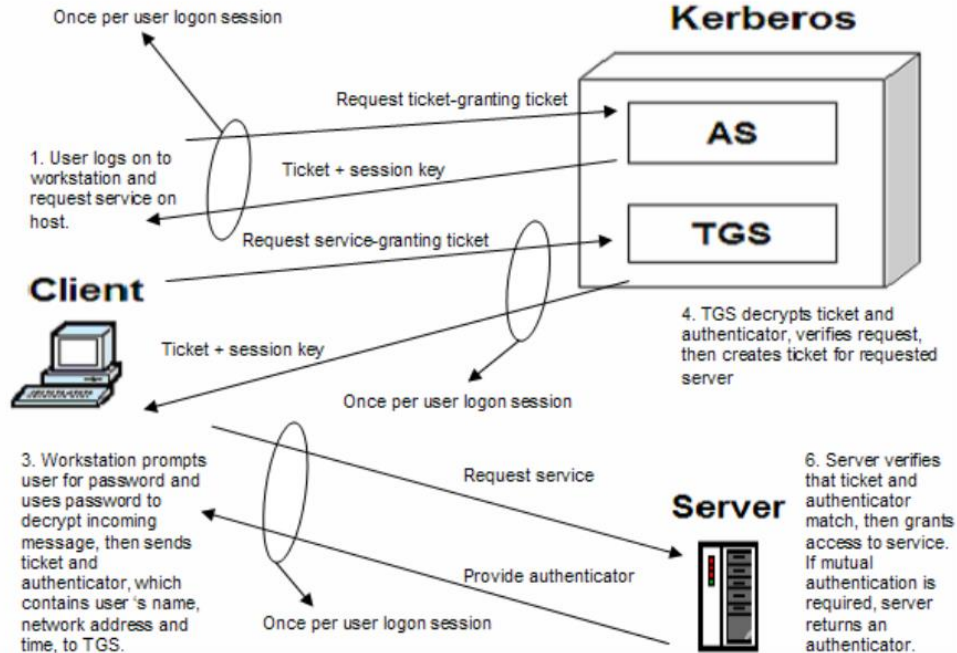


Fig. 1 Kerberos Authentication Dialogue

SOURCE: <http://user.it.uu.se/~hsander/Courses/DistributedSystems/Reports/Kerberos.pdf>

Spectrum Scale : Cloud Tiering Security

- Data is encrypted (AES 256) before it is pushed to Cloud Object Storage (on-premises or off-premises)
- Supports two types of Encryption Key Management Providers to store the encryption key
 - IBM Security Key Lifecycle Manager and Java Key Store
- TLS protocol is used when communicating with the cloud.

