SDC 20

BY Developers FOR Developers

Storage Developer Conference
September 22-23, 2020

Securing SMB3 over RDMA

Wen Xin
Microsoft Corp.

Overview

- Crypto transform over direct data placement.
- RDMA Encryption
  - Shipped in Mn (20H1) release.
  - Includes 256-bit AES algorithms.
- RDMA Signing
  - Feature complete.
  - Includes AES-GMAC algorithm.

Protocol Updates

Protocol Update - Negotiate

- RDMA_TRANSFORM_CAPABILITIES

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
TransformCount																Reserved1															
Reserved2																															
RDMATransformIds (variable)																															
...																															

Protocol Update – RDMA Channel

- SMB2_CHANNEL_RDMA_TRANSFORM

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
RdmaDescriptorOffset																RdmaDescriptorLength															
Channel																															
TransformCount																Reserved1															
Reserved2																															

Protocol Update – RDMA Encryption

- SMB2_CHANNEL_RDMA_TRANSFORM

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
TransformType																SignatureLength															
NonceLength																Reserved															
Signature (variable) Reserved1																															
...																															
Nonce (variable)																															
...																															
Padding (variable)																															

Performance

Demo