Rockin’ and Rollin’ with SMB3

Ned Pyle, Microsoft

April 5, 2017
Today’s Presenters

Ned Pyle
SMB Program Manager
Microsoft

John Kim
Chair, SNIA-ESF
Mellanox
SNIA at a glance

160
unique member companies

3,500
active contributing members

50,000
IT end users & storage pros worldwide

Learn more: snia.org/technical

© 2017 Storage Networking Industry Association. All Rights Reserved.
The material contained in this presentation is copyrighted by the SNIA unless otherwise noted.

Member companies and individual members may use this material in presentations and literature under the following conditions:

- Any slide or slides used must be reproduced in their entirety without modification.
- The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.

This presentation is a project of the SNIA.

Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.

The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.
The evolution of SMB:

- **The 1980s**: The primordial ooze
- **The 1990s**: SMB1/"CIFS"
- **Early 2000s**: SMB2
- **Past 5 years**: SMB3
- **SMB 3.1.1**:
DOS, Windows, LANMan(!)
Ubiquitously abused
Slow unsafe $%^#
Windows Vista+ / Windows Server 2008+

User-optimized

Request compounds, large reads and writes
Folder & file property caching
Durable handles
Improved message signing - HMAC SHA-256
Large MTU support
SMB 3

Windows 8+ / Windows Server 2012+
Datacenter application-optimized
Software-defined fabric
Modern user
Not CIFS. Never, ever CIFS
<table>
<thead>
<tr>
<th>Security</th>
<th>Scale</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Transparent failover</td>
<td>RDMA</td>
</tr>
<tr>
<td>Pre-auth integrity</td>
<td>Scale-out File Server</td>
<td>Multichannel</td>
</tr>
<tr>
<td>Guest block</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security
SMB Encryption & Signing

End-to-end SMB encryption

Privacy
AES-128-GCM & AES-128-CCM

SMB Signing updated

Integrity
AES-CMAC

Requires* AES-NI CPUs

Per share or server
UNC Hardening

Introduced in Win10, KB3000483

MitM prevention

Require Mutual Auth, Signing/Encryption

Client decides

Specify UNC paths to protect

Win10 defaults for AD DS

\SYSVOL
\NETLOGON
Poisoned ARP

Request \domain\netlogon\script.ps1

Serves evil \domain\netlogon\script.ps1

Serves \domain\netlogon\script.ps1

Router

Attacker

DC
Pre-authentication Integrity

MitM protection
Session Setup signed
Tree Connect encrypted
No SMB capabilities downgrade possible
Replaces “Secure negotiate”
Cannot be disabled
Update WAN accelerators

Client
- Negotiate request
- Negotiate response
- Session setup request
- Session setup response
- Session setup request
- Session setup response
- Tree connect request
- Tree connect response

Server

Unsigned/Unencrypted  Signed/Encrypted
Insecure Guest Auth

Stop Guest usage on failed auth
Bad behavior allowed by default
Because SOHO NAS

Group Policy
“Enable Insecure Guest Logons”
key="HKLM\Software\Policies\Microsoft\Windows\LanmanWorkstation"
DWORD="AllowInsecureGuestAuth"

If SMB1 enabled, meaningless
SMB3 security doesn’t matter if SMB1 is enabled
I’m sorry Mr. Johnson, but the test is positive.

Please read this pamphlet...
SMB 1

Deprecated years ago
Removable since WS2012 R2/Win8.1
Disable-able since Vista/2008
Gone in WS2016 Nano
Uninstalled by default in certain upcoming releases
Why might SMB1 still be in use?

XP & WS2003 under custom support agreement
Yeah right

Antique firmware printers
“Scan to share”

Evil NAS devices

Older Linux
Set-SmbServerConfiguration -AuditSmb1Access $true
Zap it

KB2696547
Question
break 1
Scale
SMB Transparent Failover

Failover transparent to application
Zero downtime – small IO delay during failover
Planned & unplanned failovers
Clustered

1. Normal operation
2. Failover share - connections & handles lost temporary stall of IO
   Connections & handles auto-recovered
3. Application IO continues with no errors

Hyper-V

\fs\share

File Server Cluster
SMB Scale-Out File Server

Server app storage
Example: Hyper-V and SQL Server
Increase available bandwidth by adding nodes
CSV

Key capabilities
Active/Active file shares
Fault tolerance with zero downtime
Fast failure recovery
Forced unit access/write through
Performance
SMB Multichannel

Full Throughput
Bandwidth aggregation

Automatic Failover

Automatic Configuration
SMB detects & uses multiple paths

Requires one:
One+ RSS-enabled NIC
Multiple network adapters
Teamed NICs
One+ RDMA NICs
SMB Direct (SMB over RDMA)

High throughput
Low latency
Minimal CPU
Load balancing
Automatic failover
Bandwidth aggregation

Required hardware
iWARP
RoCE v1 & V2
InfiniBand

<table>
<thead>
<tr>
<th>NIC</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>1Gb Ethernet</td>
<td>~0.1 GB/sec</td>
</tr>
<tr>
<td>10Gb Ethernet</td>
<td>~1.1 GB/sec</td>
</tr>
<tr>
<td>40Gb Ethernet</td>
<td>~4.5 GB/sec</td>
</tr>
<tr>
<td>32Gb InfiniBand (QDR)</td>
<td>~3.8 GB/sec</td>
</tr>
<tr>
<td>56Gb InfiniBand (FDR)</td>
<td>~6.5 GB/sec</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HBA</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>3Gb SAS x4</td>
<td>~1.1 GB/sec</td>
</tr>
<tr>
<td>6Gb SAS x4</td>
<td>~2.2 GB/sec</td>
</tr>
<tr>
<td>4Gb FC</td>
<td>~0.4 GB/sec</td>
</tr>
<tr>
<td>8Gb FC</td>
<td>~0.8 GB/sec</td>
</tr>
<tr>
<td>16Gb FC</td>
<td>~1.5 GB/sec</td>
</tr>
</tbody>
</table>
Question break 2
Real world examples
Storage Spaces Direct (hyper-converged storage cluster)

Hybrid

All-Flash

NVMe+SSD+HDD

SMB 3.1.1 over RDMA or TCP/IP
Storage Spaces Direct quasi-demo
Storage Spaces Direct quasi-demo
Storage Spaces Direct quasi-demo

336 virtual machines
512KB random read workload
Storage Spaces Direct quasi-demo

160 GB/s
Storage Spaces Direct quasi-demo

or 1.2+ Terabit/s
Storage Spaces Direct quasi-demo

Only 25% CPU utilization
Hyper-V Live Migration over SMB

SMB transport for Live Migration

RDMA
Multichannel over multiple NICs
Storage Replica (block replica engine for DR)

- **Applications** (local or remote)
  - Source Server Node (SR)
    - Data
    - Log
  - Destination Server Node (SR)
    - Data
    - Log

1. Application writes to Source Server Node (SR)
2. Source Server Node (SR) sends data to Destination Server Node (SR)
3. Destination Server Node (SR) receives data
4. Source Server Node (SR) sends log to Destination Server Node (SR)
5. Destination Server Node (SR) acknowledges receipt of log
SMB3 Users & Vendors

Apple
EMC
NetApp
Ryussi
Tuxera
Visuality
Etc…
SMB1 removal - aka.ms/stopusingsmb1
SOFs best practices - aka.ms/sofsyaynay
SMB & Windows Server - aka.ms/windowsserver
SMB team blog - aka.ms/serverstorage
Good SMB blog - aka.ms/josesmb3
2017 SNIA SMB3 Plugfest

- Co-located at SNIA’s Storage Developer Conference, September 11-14, Santa Clara, CA
- Enables vendors to bring their implementations of SMB3 to test, identify, and fix bugs in a collaborative setting with the goal of developing interoperable products
- 20+ companies and 80+ attendees are expected
- Evening Reception and Open House scheduled for September 11th
Final questions
After This Webcast

❖ Please rate this webcast and provide us with feedback
❖ This webcast and a PDF of the slides will be posted to the SNIA Ethernet Storage Forum (ESF) website and available on-demand
❖ [www.snia.org/forums/esf/knowledge/webcasts](http://www.snia.org/forums/esf/knowledge/webcasts)
❖ A full Q&A from this webcast, including answers to questions we couldn't get to today, will be posted to the SNIA-ESF blog: [sniaesfblog.org](http://sniaesfblog.org)
❖ Follow us on Twitter @SNIAESF
Thank you!