April 17-18, 2024
sambaXP Conference

Microsoft Interoperability Track
Next generation SMB in Windows Server 2025 & Windows
Ned Pyle
Principal Program Manager
Windows Server Engineering
Agenda

Security mindset

Coming next

Demos
Windows Server 2025 & Windows security campaign

Security 1st
Performance 2nd
Compatibility 3rd
New capabilities
SMB in Windows and Windows Server 2025

**CY 2022 releases**
- SMB Compression behavior (Aug GA)
- SMB auth rate limiter (Sep Insiders)

**CY 2023 H1 releases**
- SMB guest auth off in Pro (Jan Insiders)
- SMB1 client off in Home (Feb GA)
- SMB Mailslots disabled (Mar Insiders)
- SMB signing required (Jun Insiders)
SMB auth rate limiter

Throttle bad NTLM, PKU2U, Local KDC passwords
   Not AD-based Kerberos

2-second delay between each fail (configurable)
   On by default

Control with PowerShell, Group Policy
   Set-SmbServerConfiguration -InvalidAuthenticationDelayTimeInMs n

Ex: 300 brute force attempt/sec for 5 minutes = 90,000 PW
Now takes 50 hours
SMB auth rate limiter

Demo
SMB guest auth off in Pro

Guest auth still common in NAS
None of yours, right?

Easy method to attack phished client
Send them UNC
Allows connection without cred
User executes a remote payload

Pro defaults to off now
Only Home edition remains
SMB1 client off in Home

SMB1 usage 8 years ago: 45%
Usage now: 0.25%
That’s all, folks: SMB1 disabled in every edition
SMB Mailslots disabled

Old, simple, unreliable, insecure IPC method
SMB and AD (DCLOCATOR) mailslot disabled by default
Control with PowerShell & GP
  Set-SmbClientConfiguration -EnableMailslots $true
Officially deprecated
SMB signing required

Signing required by default now
   Previously required only for domain controller, SYSVOL, NETLOGON
   Now Windows + Windows Server
   SMB server signing required: Windows client SKUs only
   SMB client signing required: Windows and Windows Server

Stop relay attacks, AitM, phishing

Control with Powershell, Group Policy
   Don’t query registry!
SMB signing required

Errors when signing prevented:
0xc000a000 / -1073700864
STATUS_INVALID_SIGNATURE
The cryptographic signature is invalid

Performance considerations
Core speed, count & utilization
Ned tests on 4 vCPU Xenon 3.9Ghz: about -15% throughput (60 sec copy now 68 sec)
Don’t forget about SMB compression savings
Customers must test & decide
SMB signing required

The next big campaign
https://aka.ms/wontsignsmb
wontsignsmb@microsoft.com

All Windows versions support signing & it’s always enabled

Signing required by pre-auth integrity in 3.1.1
If a device or app won’t sign by default, turn it on
If you can’t turn it on, upgrade the device or app
SMB in Windows and Windows Server 2025

**CY 2022 releases**
- SMB1 client off in Home (Apr Insiders)
- SMB Compression behavior (Aug GA)
- SMB auth rate limiter (Sep Insiders)

**CY 2023 H1 releases**
- SMB guest auth off in Pro (Jan Insiders)
- SMB1 client off in Home (Feb GA)
- SMB1 Mailslots disabled (Mar Insiders)
- SMB signing required (Jun Insiders)

**CY 2023 H2 releases**
- SMB NTLM blocking option (Sep Insiders)
- SMB dialect control (Sep Insiders)
- SMB over QUIC client access control (Oct Insiders)
- SMB global encrypt from client (Oct Insiders)
- SMB firewall rule tighten (Nov Insiders)
- SMB alternative ports (Nov Insiders)
- Surprise
SMB NTLM disable option

Stop emitting NTLM secrets for PtH and offline crack
LSA change for SPNEGO that an app/service utilizes
Off by default (currently)
Remote NTLM only

Control with Powershell, Group Policy, mapping tools

```
Set-SmbClientConfiguration -DisableNTLM $true
```

Exception list in group policy, Powershell *(coming)*
SMB NTLM blocking

Demo
Phase out NTLM, use Kerberos

- IAKerb
- Local KDC
- NTLM to Nego
- IP SPN
## Kerberos Replacements for NTLM

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client lacks line-of-sight to the KDC</td>
<td>IAKerb</td>
</tr>
<tr>
<td>Workgroup / P2P / Local Auth</td>
<td>Local KDC</td>
</tr>
<tr>
<td>IP Address for target server</td>
<td>TryIPSPN</td>
</tr>
<tr>
<td>Hard-coded or unnecessary NTLM</td>
<td>Move to Nego</td>
</tr>
</tbody>
</table>
IAKerb

Initial and pass-thru authentication
Kerberos V5 and the GSS-API
New security package in existing SPNEGO
Need updated client and target
  Not DC
Kerberos mostly unchanged
IAKerb client forwards thru IAKerb target to DC
  No line of site needed by client to DC
IAKerb in action
IAKerb (with SMB)

Demo
Local KDC

- Local users and groups
- KDC without domain controller
  - On top of SAM
- Requires IAKerb-enabled client
  - No SPNs or DNS, after all
- No NTLM in Windows workgroups
- Open standards interop (in progress)
Local KDC in action

![Diagram showing the flow of AS-REQ, TGS-REQ, AP-REQ, AS-REP, TGS-REP, AP-REP messages between a client and a Windows server]
Local KDC (with SMB)

Demo
SMB server dialect control

Allow and refuse a range of SMB 2 & 3
Better security control in modern environments
Improve SMB client option introduced in Win10

PowerShell

Set-SmbClientConfiguration -Smb2DialectMax -Smb2DialectMin
Set-SmbServerConfiguration -Smb2DialectMax -Smb2DialectMin

Group policy
No need to set max!
Reintroducing: SMB over QUIC

QUIC: secure and reliable transport built on UDP
Encryption is always required
Handshake is authenticated using TLS 1.3
Does not require VPN
Runs over 443
   By default
SMB for telecommuters, mobile devices, cloud, high security
Came in Windows Server 2022 Azure Edition
SMB over QUIC

Demo
SMB over QUIC client access control

Mutual auth through certificate exchange
Allow and block specific client access
ACL based on client certificate + chain
Certificates identified by SHA256 hash or issuer name
Access granted if no deny entry + allow entry
Very granular control
  With operational overhead
SMB over QUIC mutual auth
SMB over QUIC client access control
Azure Files’ problem: ISPs blocking port 445
VPN options to Azure Files not ideal

SMB over QUIC: port 443 admin irritation

Solution: alternative ports in SMB
  SMB server: QUIC only
  SMB client: QUIC, TCP, RDMA
  Azure Files: TCP only (coming)
Configure & use SMB alternative ports

Server
New-SmbServerAlternativePort -TransportType QUIC -Port 555 -EnableInstances Default

Client
Net use Z: \contoso.azurefiles.com /tcpport:4444
New-SmbMapping -LocalPath Z: -RemotePath \srv\sales -QuicPort 3333
New-SmbGlobalMapping -RemotePath \srv\app1 -Rdmaport 2222
Always encrypt all SMB from client
Match SMB signing management
For highest security posture environments
Control with Powershell, Group Policy
SmbClientConfiguration –RequireEncryption $true
New audit option in GP
SMB firewall rule tighten

End legacy firewall rules

Installing File Server role opens
   SMB 445/5445, WMI, DCOM

Create share opens
   SMB 445/5445, ICMP, LLMNR, NetBT Datagram, NetBT Name, NetBT Session, Spooler RPC

Now: creating share doesn’t open NB 137-139

Plan: stop also opening ICMP, LLMNR, Spooler RPC
SMB over QUIC in all editions

SMB over QUIC server
- Windows Server 2025 Azure Edition
- Windows Server 2025 Datacenter
- Windows Server 2025 Standard

Free

No Arc, no subscription

Nothing up my sleeve
SMB in Windows and Windows Server 2025

CY 2023 H1 release
- SMB guest auth off in Pro (Jan Insiders)
- SMB1 client off in Home (Feb GA)
- SMB1 Mailslots disabled (Mar Insiders)
- SMB signing required (Jun Insiders)

CY 2023 H2 release
- SMB NTLM blocking option (Sep Insiders)
- SMB dialect control (Sep Insiders)
- SMB over QUIC client access control (Oct insiders)
- SMB global encrypt from client (Oct Insiders)
- SMB firewall rule tighten (Nov Insiders)
- SMB alternative ports (Nov Insiders)
- SMB over QUIC all editions (Nov Insiders)

CY 2022 release
- SMB1 client off in Home (Apr Insiders)
- SMB Compression behavior (Aug GA)
- SMB auth rate limiter (Sep Insiders)

Next major LTSC release
Next major release
- SMB guest auth off in Pro
- SMB global encrypt from client
- SMB server dialect control
- SMB signing required
- SMB auth rate limiter
- SMB NTLM disable option
- SMB over QUIC client access control
- SMB alternative ports
- SMB firewall rule tighten
- SMB Mailslots disabled
- SMB over QUIC all server editions

SMB in Windows and Windows Server 2025
Thank you!