SMB over QUIC : Sécurité et Déploiement sur Windows Server 2025

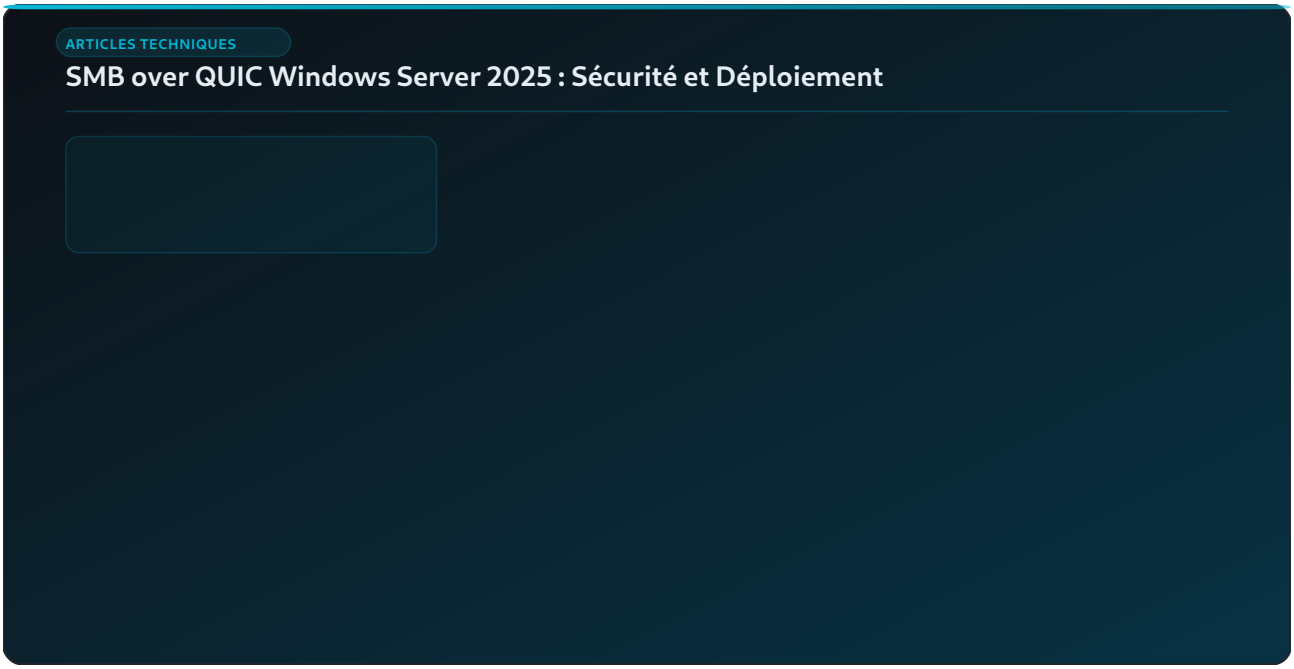
> Déployez SMB over QUIC sur Windows Server 2025 : configuration TLS 1.3, Client Access Control, Zero Trust Entra ID, conformité NIS 2 sans VPN d'entreprise.

📋 EN BREF

- SMB over QUIC permet l'accès aux partages de fichiers Windows depuis Internet via le port 443/UDP, sans VPN, grâce à TLS 1.3 intégré dans le protocole QUIC (RFC 9000).
- Windows Server 2025 supporte SMB over QUIC sur toutes les éditions (Standard et Datacenter), contrairement à Windows Server 2022 limité à l'édition Datacenter Azure Edition.
- La configuration nécessite un certificat TLS wildcard ou SAN délivré par une CA de confiance (ADCS ou CA publique) et l'ouverture du port 443/UDP sur le firewall.
- Le Client Access Control SMB over QUIC permet de restreindre finement les groupes AD autorisés à se connecter via QUIC, offrant une isolation par département ou niveau de sensibilité.
- SMB over QUIC s'intègre avec Microsoft Entra ID et le Conditional Access pour une architecture Zero Trust complète : compliance du device, MFA et vérification de l'identité avant tout accès aux fichiers.

La transformation du travail hybride en France impose aux entreprises de repenser en profondeur leurs architectures d'accès aux ressources. Les RSSI des ETI et grandes entreprises parisiennes et régionales doivent garantir l'accès sécurisé aux partages de fichiers Windows pour des milliers de

télétravailleurs, tout en réduisant la surface d'attaque exposée sur Internet. Traditionnellement, cette problématique était résolue par des VPN IPSec ou SSL — solutions efficaces mais coûteuses en licences, complexes à opérer, sources de latence et souvent contournées par les utilisateurs. SMB over QUIC, introduit dans Windows Server 2022 Datacenter Azure Edition et généralisé dans Windows Server 2025 sur toutes les éditions, représente une alternative architecturalement plus élégante : les partages SMB deviennent accessibles directement depuis Internet sur le port 443/UDP, avec TLS 1.3 intégré et une authentification Active Directory complète, sans VPN, sans latence d'établissement de tunnel et avec un déploiement opérationnel en quelques heures. Cet article propose un guide technique exhaustif de déploiement SMB over QUIC en environnement d'entreprise, couvrant la configuration, la sécurité, le monitoring et la conformité NIS 2 pour les entreprises françaises engagées dans une démarche Zero Trust.



QUIC (Quick UDP Internet Connections), standardisé par la RFC 9000 en mai 2021, est un protocole de transport multiplexé fonctionnant sur UDP avec TLS 1.3 intégré. Il a été conçu par Google pour accélérer les connexions web (HTTP/3 repose sur QUIC) et apporte plusieurs avantages fondamentaux par rapport à TCP+TLS pour les accès distants.

QUIC (RFC 9000) : les avantages techniques

QUIC adresse plusieurs limitations de TCP qui affectent les performances des accès distants :

0-RTT ou 1-RTT handshake : TLS 1.3 intégré dans QUIC permet d'établir une connexion sécurisée en 1 aller-retour (contre 3 pour TCP+TLS 1.2), voire 0-RTT pour les reconnexions vers des serveurs déjà connus

Multiplexage sans head-of-line blocking : Plusieurs flux de données peuvent coexister dans une même connexion QUIC sans qu'un paquet perdu sur un flux ne bloque les autres (contrairement à TCP)

Migration de connexion : Un client changeant de réseau (WiFi vers 4G) peut maintenir sa connexion QUIC active sans reconnexion grâce aux Connection IDs

NAT traversal natif : QUIC fonctionne sur UDP, mieux supporté par les NAT que certains protocoles VPN

TLS 1.3 obligatoire : Pas de fallback vers des versions TLS plus anciennes et vulnérables

SMB over QUIC vs VPN : comparatif

Critère	VPN IPSec/SSL traditionnel	SMB over QUIC
Protocole de transport	UDP (IPSec) / TCP+TLS (SSL)	UDP + TLS 1.3 intégré (QUIC)
Port utilisé	500/UDP, 4500/UDP (IPSec) ou 443/TCP (SSL)	443/UDP
Latence d'établissement	2-5 secondes (tunnel + authentification)	100-300 ms (1-RTT QUIC + Kerberos)
Accès granulaire	Non (accès réseau global)	Oui (par partage SMB, par groupe AD)
Client requis	Client VPN dédié (AnyConnect, GlobalProtect, etc.)	Natif Windows 11 (aucun client additionnel)
Split tunneling	Configuration complexe, risques	Natif (seul le trafic SMB est concerné)
Coût de licences	Élevé (concentrateur VPN + licences)	Inclus dans Windows Server 2025
Zero Trust natif	Non (accès réseau large)	Oui (accès fichier uniquement, Entra ID)

Cas d'usage : télétravail sans VPN

SMB over QUIC est particulièrement adapté aux scénarios suivants en entreprise française :

Télétravail régulier : Accès aux serveurs de fichiers internes depuis le domicile sans déployer un client VPN

Postes nomades commerciaux : Commerciaux accédant aux partages depuis des hôtels ou bureaux clients

Accès depuis des appareils non joints au domaine : Postes personnels autorisés accédant à des partages spécifiques

Filiales sans VPN site-à-site : Petites filiales distantes accédant aux serveurs de fichiers du siège

Réduction de la surface VPN : Migration progressive du VPN vers SMB over QUIC pour les cas d'usage fichiers

---

Prérequis et Architecture SMB over QUIC

Avant de déployer SMB over QUIC, vérifiez la compatibilité des différents composants de votre infrastructure. Les prérequis sont stricts et non négociables.

> ⚡ **Retour terrain**
>
> Pour un éditeur SaaS RH qui migrait vers Kubernetes, la première mise en production a révélé des pods qui consommaient 10× plus de mémoire que prévu — sans limits configurées, ils saturaient les nodes. J'avais prévenu que les limits et requests devaient être calibrées avant le départ en production. La leçon retenue : dans un cluster mutualisé, un pod sans limite est une bombe à retardement pour les voisins.

Prérequis côté serveur

La disponibilité de SMB over QUIC côté serveur dépend de la version et de l'édition Windows Server :

Windows Server 2022 Datacenter Azure Edition uniquement : SMB over QUIC disponible, mais uniquement pour les instances Azure ou Azure Stack HCI. Non disponible sur les serveurs on-premises Standard ou Datacenter non-Azure.

Windows Server 2025 Standard et Datacenter : SMB over QUIC disponible sur toutes les éditions, y compris les serveurs on-premises. C'est la configuration recommandée pour les entreprises françaises.

File Server role : Le rôle Serveur de fichiers doit être installé (`Install-WindowsFeature FS-FileServer`)

Certificat TLS requis

SMB over QUIC requiert un certificat TLS valide sur le serveur. Ce certificat doit répondre aux critères suivants :

Émis par une CA approuvée par les clients (ADCS d'entreprise ou CA publique comme DigiCert, Sectigo)

Inclure le FQDN du serveur dans le Subject Alternative Name (SAN) : `fileserver.entreprise.fr`

Ou utiliser un certificat wildcard : `*.entreprise.fr`

Algorithme RSA 2048 bits minimum, ou EC P-256/P-384

Période de validité non expirée

Pour les accès depuis Internet (hors domaine AD), il est recommandé d'utiliser une CA publique dont le certificat racine est présent dans le Windows Certificate Store de tous les clients, y compris les postes non joints au domaine. Pour les accès exclusivement depuis des postes membres du domaine, l'ADCS d'entreprise suffit.

Clients supportés

Windows 11 (toutes éditions) : Support natif complet de SMB over QUIC client

Windows 10 version 22H2 et ultérieur : Support SMB over QUIC client (avec KB approprié)

Windows Server 2022 / 2025 : Peuvent agir comme clients SMB over QUIC

Clients Linux, macOS : Non supportés nativement (SMB over QUIC est une extension Microsoft)

Architecture réseau

Le port 443/UDP doit être ouvert sur le firewall périmétrique en entrée vers le serveur de fichiers (ou vers un load balancer/reverse proxy en frontal). Contrairement aux idées reçues, QUIC/UDP 443 est généralement autorisé par les firewalls des hôtels et espaces de coworking, qui bloquent les ports VPN classiques (1194/UDP pour OpenVPN, 500/UDP et 4500/UDP pour IPSec) mais laissent passer le port 443 quel que soit le protocole de couche transport (TCP ou UDP).

Configuration de SMB over QUIC sur Windows Server 2025

La configuration de SMB over QUIC sur Windows Server 2025 se fait entièrement via PowerShell. Voici les étapes complètes de déploiement.

Activation de SMB over QUIC

```
 # Verifier la version Windows Server (doit etre 2025 ou 2022 Datacenter Azure Edition)
Get-ComputerInfo | Select-Object WindowsProductName, OsVersion

# Verifier que le role File Server est installe
Get-WindowsFeature FS-FileServer

# Activer SMB over QUIC
Enable-SmbServerConfiguration -EnableSMBQUIC $true

# Verifier l'etat de SMB over QUIC
Get-SmbServerConfiguration | Select-Object EnableSMBQUIC
```

Attribution du certificat TLS

```
 # Lister les certificats disponibles dans le store LocalMachine\My
Get-ChildItem Cert:\LocalMachine\My | Select-Object Subject, Thumbprint, NotAfter |
    Where-Object { $_.NotAfter -gt (Get-Date) } | Format-Table

# Recuperer l'empreinte du certificat pour le serveur de fichiers
$cert = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
    ($_.Subject -like "*fileserver.entreprise.fr*" -or
     $_.Subject -like "*.entreprise.fr*") -and
    $_.NotAfter -gt (Get-Date)
} | Sort-Object NotAfter -Descending | Select-Object -First 1

Write-Host "Certificat selectionne : $($cert.Subject) - Expire : $($cert.NotAfter)"

# Creer le mapping certificat pour SMB over QUIC
New-SmbServerCertificateMapping `
    -Name "QuicCertificate" `
    -Thumbprint $cert.Thumbprint `
    -StoreName My

# Verifier le mapping
Get-SmbServerCertificateMapping
```

Script PowerShell complet de configuration SMB over QUIC

```
 # Script complet de configuration SMB over QUIC - Windows Server 2025
# Prerequis : Certificat TLS valide dans Cert:\LocalMachine\My

param(
    [Parameter(Mandatory)]
    [string]$CertificateFQDN,      # Ex: "fileserver.entreprise.fr"

    [string]$MappingName = "SmbQuicCert",

    [switch]$RequireSignature = $true,

    [switch]$RequireEncryption = $true
)

# 1. Verifier la compatibilite OS
$osInfo = Get-ComputerInfo
if ($osInfo.OsVersion -lt "10.0.20348") {
    Write-Error "SMB over QUIC requiert Windows Server 2022+ (Datacenter Azure) ou Windows Server
    exit 1
}

# 2. Activer SMB over QUIC
Enable-SmbServerConfiguration -EnableSMBQUIC $true -Force
Write-Host "[OK] SMB over QUIC active"

# 3. Configurer le SMB signing et encryption (securite renforcee)
Set-SmbServerConfiguration `
    -RequireSecuritySignature $RequireSignature `
    -EncryptData $RequireEncryption `
    -Force
Write-Host "[OK] SMB signing et encryption configures"

# 4. Recuperer et mapper le certificat TLS
$cert = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
    ($_.Subject -like "*$CertificateFQDN*" -or
     $_.Extensions | Where-Object {
         $_.Oid.Value -eq "2.5.29.17" -and $_.Format(0) -like "*$CertificateFQDN*"
     }) -and $_.NotAfter -gt (Get-Date)
} | Sort-Object NotAfter -Descending | Select-Object -First 1

if (-not $cert) {
    Write-Error "Aucun certificat valide trouve pour $CertificateFQDN"
    exit 1
}
```

```
# Supprimer l'ancien mapping si existant
Remove-SmbServerCertificateMapping -Name $MappingName -ErrorAction SilentlyContinue

New-SmbServerCertificateMapping `
    -Name $MappingName `
    -Thumbprint $cert.Thumbprint `
    -StoreName My
Write-Host "[OK] Certificat mappe : $($cert.Subject) (expire: $($cert.NotAfter))"

# 5. Configurer le pare-feu Windows pour QUIC
New-NetFirewallRule `
    -DisplayName "SMB over QUIC - Entrant 443/UDP" `
    -Direction Inbound `
    -Protocol UDP `
    -LocalPort 443 `
    -Action Allow `
    -Profile Domain,Private `
    -Enabled True `
    -ErrorAction SilentlyContinue
Write-Host "[OK] Regle pare-feu creee pour 443/UDP"

# 6. Resume de la configuration
Write-Host "`n=== Configuration SMB over QUIC ==="
Get-SmbServerConfiguration | Select-Object EnableSMBQUIC, RequireSecuritySignature, EncryptData
Get-SmbServerCertificateMapping | Format-Table Name, Thumbprint, StoreName
```

Contrôle d'Accès SMB over QUIC : Client Access Control

Une des fonctionnalités les plus importantes de SMB over QUIC en entreprise est le Client Access Control, qui permet de définir précisément quels comptes ou groupes Active Directory sont autorisés à se connecter via QUIC. Cette granularité est essentielle pour une architecture Zero Trust.

New-SmbClientAccessControl : configuration granulaire

```
 # Lister les regles d'acces QUIC existantes
Get-SmbClientAccessControl

# Autoriser un groupe AD specifique pour SMB over QUIC
# Exemple : autoriser uniquement le groupe "FS-QUIC-Authorized"
New-SmbClientAccessControl `
    -IdentifierType SDDL `
    -Identifier "D:(A;;0x1200a9;;;S-1-12-1-XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX)" `
    -AccessControlType Allow

# Alternative : specifier par nom de groupe (necessite traduction en SID)
$groupSID = (Get-ADGroup "FS-QUIC-Authorized").SID.Value
New-SmbClientAccessControl `
    -IdentifierType SDDL `
    -Identifier "D:(A;;0x1200a9;;;$groupSID)" `
    -AccessControlType Allow

# Bloquer explicitement un groupe (ex: comptes de service)
$svcSID = (Get-ADGroup "Service-Accounts").SID.Value
New-SmbClientAccessControl `
    -IdentifierType SDDL `
    -Identifier "D:(D;;0x1200a9;;;$svcSID)" `
    -AccessControlType Deny
```

Isolation par département via Client Access Control

En entreprise, il est recommandé de créer des groupes AD dédiés par département ou niveau de sensibilité des données et de les mapper aux règles Client Access Control SMB over QUIC :

```
 # Structure de groupes AD recommandee pour SMB over QUIC
# FS-QUIC-Finances : acces QUIC pour le departement Finance
# FS-QUIC-RH : acces QUIC pour les RH
# FS-QUIC-Cadres : acces QUIC pour les cadres
# FS-QUIC-IT : acces QUIC pour l'equipe IT (acces etendu)

# Creation des regles pour chaque groupe
$groups = @("FS-QUIC-Finances", "FS-QUIC-RH", "FS-QUIC-Cadres", "FS-QUIC-IT")
foreach ($groupName in $groups) {
    try {
        $sid = (Get-ADGroup $groupName).SID.Value
        New-SmbClientAccessControl `
            -IdentifierType SDDL `
            -Identifier "D:(A;;0x1200a9;;;$sid)" `
            -AccessControlType Allow
        Write-Host "Acces QUIC autorise pour le groupe : $groupName"
    } catch {
        Write-Warning "Groupe introuvable : $groupName"
    }
}
```

Audit des connexions QUIC

```
 # Lister les sessions SMB actives via QUIC
Get-SmbSession | Where-Object { $_.TransportType -eq "QUIC" } |
    Select-Object ClientComputerName, ClientUserName, ConnectedTime, TransportType |
    Format-Table -AutoSize

# Historique des connexions via le journal d'evenements
Get-WinEvent -LogName "Microsoft-Windows-SMBServer/Operational" |
    Where-Object { $_.Id -in @(551, 553) } |
    Select-Object TimeCreated, Message |
    Format-List
```

Sécurité SMB over QUIC : Chiffrement et Authentification

SMB over QUIC offre une sécurité renforcée par rapport aux accès SMB classiques, grâce à la combinaison de plusieurs couches de protection. Comprendre ces couches est essentiel pour configurer correctement la solution et répondre aux exigences de sécurité.

TLS 1.3 obligatoire dans QUIC

Le protocole QUIC impose TLS 1.3 comme unique version TLS supportée. Il n'y a pas de fallback possible vers TLS 1.2, TLS 1.1 ou SSL 3.0, éliminant les vulnérabilités liées aux négociations vers des versions inférieures (attaques POODLE, BEAST, DROWN). TLS 1.3 apporte :

Forward Secrecy systématique (ECDHE uniquement pour l'échange de clés)

Chiffrement authentifié (AEAD : AES-128-GCM, AES-256-GCM, ChaCha20-Poly1305)

Réduction des cipher suites négociables (suppression des suites RSA statiques)

0-RTT possible pour les reconnexions (avec précautions sur le replay)

SMB signing + SMB encryption over QUIC : double couche

SMB over QUIC ajoute une couche de sécurité supplémentaire : les données SMB peuvent être à la fois chiffrées par TLS 1.3 (niveau QUIC) et signées/chiffrées par SMB 3.1.1 (niveau SMB). Cette double couche est optionnelle mais recommandée pour les données sensibles :

```
 # Activer le chiffrement SMB 3.1.1 sur le serveur (toutes connexions)
Set-SmbServerConfiguration -EncryptData $true -Force

# Activer le chiffrement sur un partage specifique uniquement
Set-SmbShare -Name "Finances" -EncryptData $true

# Activer le SMB signing obligatoire
Set-SmbServerConfiguration -RequireSecuritySignature $true -Force

# Verifier les algorithmes de chiffrement supportes (SMB 3.1.1)
Get-SmbServerConfiguration | Select-Object *Encrypt*, *Sign*
```

Authentification Kerberos et NTLM sur QUIC

L'authentification SMB over QUIC utilise les mêmes mécanismes que SMB classique : Kerberos est utilisé en priorité pour les comptes membres du domaine Active Directory, NTLM en fallback pour les comptes locaux ou les postes non joints au domaine. Il est recommandé de :

Désactiver NTLM LM et NTLMv1 via GPO (`Network security: LAN Manager authentication level = NTLMv2 only`)

Activer le SMB signing pour empêcher les attaques NTLM relay même sur connexions QUIC

Préférer Kerberos sur les postes membres du domaine (configuration correcte du DNS/SPN)

Désactiver SMBv1 avant déploiement QUIC

SMBv1 est une condition bloquante : il doit être désactivé avant de déployer SMB over QUIC pour éviter tout downgrade attack. SMBv1 est vulnérable à EternalBlue (MS17-010), utilisé notamment par WannaCry et NotPetya.

```
 # Verifier l'etat de SMBv1 sur le serveur
Get-SmbServerConfiguration | Select-Object EnableSMB1Protocol

# Desactiver SMBv1 sur le serveur
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force

# Verifier via les features Windows
Get-WindowsFeature FS-SMB1

# Desactiver la feature SMBv1 (plus radical et recommande)
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart

# Audit des clients utilisant encore SMBv1
Get-SmbSession | Where-Object Dialect -eq "1.0" | Select-Object ClientComputerName
```

Pour une configuration complète des mécanismes d'authentification Active Directory liés à SMB, voir notre article sur LDAP Signing et Channel Binding dans Active Directory.

Performance et Optimisation SMB over QUIC

Les performances de SMB over QUIC dépendent de plusieurs facteurs : l'algorithme de contrôle de congestion QUIC, la compression SMB 3.1.1 et les caractéristiques du réseau sous-jacent. Voici les paramètres d'optimisation disponibles.

Congestion control QUIC : BBR vs CUBIC

Windows Server 2025 implémente QUIC via la bibliothèque MsQuic, qui supporte plusieurs algorithmes de contrôle de congestion :

CUBIC : Algorithme par défaut, optimisé pour les réseaux à haute bande passante, peut être moins efficace sur les réseaux à longue distance (intercontinentaux)

BBR (Bottleneck Bandwidth and RTT) : Algorithme Google, mieux adapté aux réseaux avec perte de paquets, souvent plus performant pour les accès depuis des réseaux mobiles ou dégradés

```
 # Verifier la configuration QUIC actuelle
Get-SmbServerConfiguration | Select-Object *QUIC*

# Les parametres de congestion control sont geres par MsQuic
# Verifier la version MsQuic installee
Get-Item "C:\Windows\System32\msquic.dll" | Select-Object VersionInfo
```

Compression SMB 3.1.1

SMB 3.1.1 supporte la compression des données avant transmission, réduisant la bande passante consommée pour les fichiers compressibles (documents Office, texte, XML). La compression peut être activée avec LZ77 (compatibilité maximale) ou LZ4 (meilleure performance) :

```
 # Verifier les algorithmes de compression supportes
Get-SmbServerConfiguration | Select-Object *Compress*

# Activer la compression SMB sur le serveur
Set-SmbServerConfiguration -EnableSMBCompression $true -Force

# Sur le client, verifier les algorithmes de compression supportes
Get-SmbClientConfiguration | Select-Object *Compress*

# Tester la compression sur un transfert
Copy-Item -Path "C:\TestFile.docx" -Destination "\\fileserver.entreprise.fr\share\TestFile.docx" -
```

RDMA/SMB Direct et QUIC

Il est important de noter que **RDMA/SMB Direct n'est pas compatible avec SMB over QUIC**. RDMA (Remote Direct Memory Access) permet des transferts SMB avec latence ultra-faible en mode kernel bypass, mais nécessite une infrastructure réseau spécialisée (RoCE, InfiniBand) disponible uniquement sur des réseaux locaux. Pour les accès QUIC depuis Internet, le transport est QUIC sur UDP, et SMB Direct ne s'applique pas. Les benchmarks réalistes pour SMB over QUIC sur des connexions entreprise (100 Mbps symétriques) montrent des débits de 60-80 Mbps, comparables à une connexion VPN SSL bien configurée mais avec une latence d'établissement nettement inférieure.

Monitoring SMB over QUIC

La supervision de SMB over QUIC est essentielle pour détecter les connexions suspectes, les tentatives d'accès non autorisées et les anomalies de performance.

Event IDs SMB over QUIC

Les événements SMB over QUIC sont journalisés dans les journaux d'événements Windows sous `Microsoft-Windows-SMBServer/Operational` et `Microsoft-Windows-SMBServer/Security`. Les Event IDs pertinents sont :

Event ID 551 : Connexion SMB over QUIC établie (succès)

Event ID 553 : Tentative de connexion SMB over QUIC rejetée par Client Access Control

Event ID 1 : Service SMB Server démarré

Event ID 3 : Service SMB Server arrêté

Event ID 14 : Erreur de certificat TLS lors d'une connexion QUIC

Event ID 30001 : QUIC connection established

Event ID 30002 : QUIC connection closed

Event ID 30003 : QUIC connection error

```
 # Monitorer les connexions QUIC en temps reel
Get-WinEvent -LogName "Microsoft-Windows-SMBServer/Operational" -MaxEvents 100 |
    Where-Object { $_.Id -in @(551, 553, 30001, 30002, 30003) } |
    Select-Object TimeCreated, Id, Message |
    Format-List

# Sessions SMB QUIC actives
Get-SmbSession | Where-Object { $_.Dialect -eq "3.1.1" } |
    Select-Object ClientComputerName, ClientUserName, ConnectedTime, NumOpens |
    Format-Table -AutoSize

# Compter les connexions QUIC par utilisateur
Get-SmbSession | Where-Object { $_.TransportType -eq "QUIC" } |
    Group-Object ClientUserName |
    Sort-Object Count -Descending |
    Format-Table Name, Count
```

Performance counters SMB

```
 # Compteurs de performance SMB disponibles
Get-Counter -ListSet "SMB Server" | Select-Object -ExpandProperty Counter | Where-Object { $_ -lik

# Surveiller les performances SMB en temps reel
$counters = @(
    "\SMB Server\Bytes/sec",
    "\SMB Server\Read Requests/sec",
    "\SMB Server\Write Requests/sec",
    "\SMB Server\Connections"
)
Get-Counter -Counter $counters -SampleInterval 5 -MaxSamples 12
```

Wazuh : détection de connexions QUIC suspectes

Les règles Wazuh suivantes permettent de détecter les anomalies sur les connexions SMB over QUIC, en s'appuyant sur les Event IDs Windows collectés via l'agent Wazuh :

```
 <!-- Regle Wazuh : connexion SMB QUIC rejetee (acces non autorise) -->
<rule id="100551" level="10">
    <if_sid>60103</if_sid>
    <field name="win.system.eventID">553</field>
    <description>SMB over QUIC : tentative connexion rejetee par Client Access Control</descriptio
    <group>smb,quic,access_denied</group>
</rule>

<!-- Regle Wazuh : erreur certificat TLS sur connexion QUIC -->
<rule id="100552" level="12">
    <if_sid>60103</if_sid>
    <field name="win.system.eventID">14</field>
    <description>SMB over QUIC : erreur certificat TLS - possible attaque MITM</description>
    <group>smb,quic,tls_error</group>
</rule>
```

Pour une visibilité complète sur les événements Active Directory liés aux sessions de fichiers, consultez notre guide sur les Authentication Silos dans Windows Server 2025.

SMB over QUIC et Zero Trust : Intégration avec Entra ID

SMB over QUIC s'intègre naturellement dans une architecture Zero Trust lorsqu'il est combiné avec Microsoft Entra ID (anciennement Azure AD) et les fonctionnalités de Conditional Access. Cette intégration permet de vérifier non seulement l'identité de l'utilisateur mais aussi la conformité du device avant d'autoriser l'accès aux partages de fichiers.

Conditional Access sur SMB over QUIC via Entra ID

L'intégration Entra ID pour SMB over QUIC fonctionne via le mécanisme d'authentification moderne combiné à la jointure hybride Azure AD ou à la jointure Azure AD directe des postes Windows 11 :

```
 # Verifier que le poste est joint a Azure AD (hybride ou direct)
dsregcmd /status | Select-String "AzureAdJoined|HybridAzureAdJoined|WorkplaceJoined"

# Pour les postes hybrides : verifier le token Azure AD
dsregcmd /status | Select-String "AzureAdPrt|AzureAdPrtAuthority"
```

Dans le portail Entra ID, créer une politique de Conditional Access ciblant les ressources de stockage de fichiers (Azure Files ou, pour les serveurs on-premises, via l'intégration Microsoft Entra Kerberos) :

Conditions utilisateurs : Groupes AD autorisés à utiliser SMB over QUIC

Conditions device : Device compliance (Intune) ou Hybrid Azure AD Joined

Contrôles d'accès : MFA requis pour les accès depuis des réseaux non identifiés

Session : Fréquence de reauthentification (ex: 1 heure pour les accès depuis Internet)

Device compliance check avant connexion QUIC

```
 # Verifier la compliance du device via PowerShell (Intune Graph API)
# Necessite le module Microsoft.Graph.DeviceManagement
Connect-MgGraph -Scopes "DeviceManagementManagedDevices.Read.All"

$deviceName = $env:COMPUTERNAME
$device = Get-MgDeviceManagementManagedDevice -Filter "deviceName eq '$deviceName'"
Write-Host "Compliance : $($device.ComplianceState)"
Write-Host "Derniere sync Intune : $($device.LastSyncDateTime)"
```

Intégration avec Windows Defender Application Control (WDAC)

WDAC peut être utilisé pour restreindre les applications autorisées à effectuer des connexions SMB over QUIC. En définissant une politique WDAC qui n'autorise que les applications signées par des éditeurs de confiance, on empêche les malwares d'utiliser SMB over QUIC comme canal d'exfiltration ou de déplacement latéral. Pour une configuration complète de Credential Guard en lien avec les accès distants, consultez notre article sur Credential Guard dans Windows Server 2025.

Conformité NIS 2 : Accès Distants Sécurisés pour Entreprises Françaises

SMB over QUIC s'inscrit directement dans les exigences de sécurité pour les accès distants définies par la directive NIS 2 et les recommandations de l'ANSSI pour les entreprises françaises engagées dans une transformation numérique incluant le télétravail.

NIS 2 Article 21§2.h : politiques d'accès distant

L'article 21§2.h de NIS 2 impose aux entités essentielles et importantes de mettre en oeuvre des « politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du

chiffrement ». Il requiert également des mesures pour « la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs ». SMB over QUIC répond à ces exigences :

Cryptographie forte : TLS 1.3 + SMB 3.1.1 encryption (AES-256-GCM)

Contrôle d'accès granulaire : Client Access Control par groupe AD, Conditional Access Entra ID

Traçabilité : Journalisation des connexions QUIC dans le journal d'événements Windows et le SIEM

Authentification forte : Kerberos + MFA via Entra ID pour les accès depuis Internet

Recommandations ANSSI : télétravail sécurisé

L'ANSSI a publié plusieurs guides sur la sécurité du télétravail, notamment le guide ANSSI-PA-084 « Recommandations sur le nomadisme numérique ». SMB over QUIC s'aligne sur les principes directeurs de ce guide :

Chiffrement de bout en bout des données en transit (TLS 1.3)

Authentification forte de l'utilisateur et du poste

Principe du moindre privilège (accès uniquement aux partages nécessaires)

Journalisation et supervision des accès distants

Cloisonnement des flux (SMB over QUIC ne donne accès qu'aux partages fichiers, pas au réseau interne)

Contexte ETI/PME françaises en télétravail

Pour les ETI (Entreprises de Taille Intermédiaire) et PME françaises, SMB over QUIC représente une opportunité de simplifier leur infrastructure d'accès distant tout en renforçant la sécurité. Les bénéfices opérationnels sont significatifs :

Réduction des coûts : Suppression ou réduction du concentrateur VPN (matériel ou cloud), des licences client VPN

Simplification du support : Plus de tickets « VPN ne fonctionne pas depuis l'hôtel » — QUIC/UDP 443 passe partout

Amélioration de l'expérience utilisateur : Accès instantané aux fichiers, sans délai d'établissement du tunnel VPN

Réduction de la surface d'attaque : Accès granulaire aux seuls partages de fichiers autorisés, pas d'accès réseau large comme avec un VPN

Il est recommandé de documenter le déploiement SMB over QUIC dans la Politique de Sécurité des Systèmes d'Information (PSSI) de l'entreprise, notamment les contrôles d'accès mis en place, les procédures de monitoring et les modalités de révocation en cas d'incident. Cette documentation est indispensable pour répondre aux exigences de NIS 2 en matière de gouvernance et de traçabilité. Pour des aspects complémentaires sur la sécurité AD liée à SMB, consultez notre article sur DNS over HTTPS en entreprise avec Microsoft 2026 pour une approche globale de la sécurité des protocoles réseau Microsoft.

Questions fréquentes sur SMB over QUIC

SMB over QUIC remplace-t-il complètement le VPN en entreprise ?

SMB over QUIC remplace le VPN uniquement pour les cas d'usage d'accès aux partages de fichiers Windows. Il ne fournit pas un accès réseau général : les applications nécessitant une connectivité réseau étendue (applications métier non-web, RDP direct, etc.) continuent de nécessiter un VPN. L'approche recommandée est une coexistence : SMB over QUIC pour les fichiers, ZTNA (Zero Trust Network Access) pour les autres applications.

Peut-on utiliser SMB over QUIC avec des serveurs de fichiers en cluster (SOFS) ?

Oui, SMB over QUIC est compatible avec les Scale-Out File Servers (SOFS) sur Windows Server 2025 / Azure Stack HCI. La configuration est similaire, avec le certificat TLS mappé sur le nom de réseau du cluster plutôt que sur un serveur individuel. Le Client Access Control s'applique au niveau du cluster et affecte toutes les connexions QUIC vers les noeuds du cluster.

Quel est l'impact de SMB over QUIC sur les performances de transfert de fichiers volumineux ?

Pour les transferts de fichiers volumineux (plusieurs Go), les performances de SMB over QUIC sont comparables à SMB over TCP avec TLS. Le principal avantage de QUIC concerne la latence d'établissement et la résilience aux changements de réseau, pas le débit brut. La compression SMB 3.1.1 peut améliorer significativement le débit effectif pour les fichiers compressibles. RDMA/SMB Direct n'étant pas disponible avec QUIC, les transferts ultra-rapides (100 Gbps sur réseau local) ne sont pas possibles.

Comment révoquer l'accès QUIC d'un utilisateur compromis ?

La révocation est immédiate via plusieurs mécanismes : désactiver le compte AD (les sessions Kerberos existantes expirent dans l'heure), le retirer du groupe autorisé dans Client Access Control (effet au prochain renouvellement du token), ou via une politique Conditional Access Entra ID (révocation en quelques minutes). Pour une révocation d'urgence immédiate, utiliser `Close-SmbSession` sur le serveur de fichiers pour terminer les sessions actives.

SMB over QUIC est-il vulnérable aux attaques NTLM relay ?

SMB over QUIC avec SMB signing activé (requis par défaut) n'est pas vulnérable aux attaques NTLM relay classiques. Le SMB signing intégré dans SMB 3.1.1 garantit l'intégrité de chaque message SMB. De plus, TLS 1.3 dans QUIC offre une protection channel binding, empêchant les attaques par relais de session TLS. Il est néanmoins recommandé de désactiver NTLM LM/v1 et de préférer Kerberos pour les comptes membres du domaine.

À RETENIR

À retenir

SMB over QUIC est disponible sur toutes les éditions de Windows Server 2025 (Standard et Datacenter), permettant l'accès aux partages de fichiers depuis Internet sur le port 443/UDP sans VPN, avec TLS 1.3 intégré.

La configuration requiert trois étapes : activer QUIC (`Enable-SmbServerConfiguration -EnableSMBQUIC $true`), mapper le certificat TLS (`New-SmbServerCertificateMapping`), et configurer le Client Access Control pour restreindre les groupes AD autorisés.

Désactiver SMBv1 est un prérequis obligatoire avant tout déploiement SMB over QUIC pour éliminer les vecteurs de downgrade attack.

L'intégration avec Microsoft Entra ID et Conditional Access permet une architecture Zero Trust complète : vérification de l'identité, compliance du device et MFA avant tout accès aux fichiers depuis Internet.

SMB over QUIC répond aux exigences NIS 2 Article 21§2.h sur les politiques d'accès distant chiffré et s'aligne sur les recommandations ANSSI pour le nomadisme numérique sécurisé des entreprises françaises.

Sources

ANSSI CERT-FR — Publications et alertes

MITRE ATT&CK — Framework des techniques d'attaque

CISA — Advisories de cybersécurité

