Technical Report

# SMB Protocol Best Practices

## ONTAP 9.x

John Lantz, NetApp

October 2016 | TR-4543

## Abstract

This technical report details NetApp® ONTAP® support for SMB protocol features. Functionality is covered in terms of capabilities, requirements, implementation, and best practices.

## Information Classification

Public

# Version History

| Version | Date | Document Version History |
|---|---|---|
| Version 1.1 | October 2016 | John Lantz<br>ONTAP 9.1 adds support for AES-128-GCM encryption and domain controller SMB connections. |
| Version 1.0 | August 2016 | John Lantz<br>New for ONTAP 9.<br>Covers SMB features supported by ONTAP 9. |

TABLE OF CONTENTS

Version History .......... 2

1 Overview .......... 4

1.1 CIFS or SMB? .......... 4

1.2 SMB and Windows File Services .......... 4

2 SMB 1 .......... 4

2.1 Planning for SMB Deprecation in ONTAP .......... 5

2.2 Infinite Volumes .......... 5

3 SMB 2 .......... 5

3.1 Durable Handles .......... 6

3.2 SMB Signing .......... 7

3.3 SMB 2 Unsupported Features .......... 8

4 SMB 2.1 .......... 8

4.1 Lease Oplocks .......... 8

4.2 Large MTU .......... 9

4.3 SMB 2.1 Unsupported Features .......... 10

5 SMB 3 .......... 10

5.1 Continuous Available Shares .......... 11

5.2 Scale-Out .......... 12

5.3 Transparent Failover .......... 13

5.4 Witness .......... 13

5.5 Persistent Handles .......... 14

5.6 AES-128-CCM Encryption .......... 15

5.7 SMB 3 Unsupported Features .......... 16

6 SMB 3.1.1 .......... 16

6.1 Preauthentication Integrity .......... 16

6.2 AES-128-GCM Encryption .......... 17

6.3 SMB 3.1.1 Unsupported Features .......... 18

Additional Resources .......... 18

Contact Us .......... 19

# 1 Overview

This technical report is primarily about best practices for using Microsoft's Server Message Block (SMB) protocol in ONTAP 9. SMB's low cost, ease of deployment, ease of administration, and rich integration with Windows Server and Active Directory make it the default file-sharing protocol for Windows and Macs.

SMB has traditionally been associated with general information work (file shares) but has increasingly become associated with application data and continuously available scale-out file server (SOFS) solutions (particularly Hyper-V and SQL) since the release of SMB 3.

## 1.1 CIFS or SMB?

In this technical report, the term SMB refers to modern dialects of the Common Internet File System (CIFS) protocol, specifically SMB 1, 2, and 3.

CIFS was the network file-sharing protocol for Windows NT. Given its importance and widespread use, the name stuck, and CIFS became a colloquialism for all versions of the protocol as well as the file servers, shares, and Windows file services in general.

**Interesting note:** Although CIFS predates SMB 1, 2, and so on, it doesn't predate the SMB protocol. CIFS is a dialect of SMB, an even earlier file-sharing protocol used by NetBIOS.

## 1.2 SMB and Windows File Services

Documents containing best practices associated with file servers, shares, security, Hyper-V over SMB, SQL over SMB, FPolicy, and other Windows file services that use the SMB protocol can be found in the Additional Resources section.

# 2 SMB 1

Compared to more modern SMB releases, SMB 1 is slow, not suited to nondisruptive operations, and a security risk due to its use of the now-compromised MD5 hashing algorithm.

Extended support for Windows Server 2003, the last version of Windows Server to support only SMB 1, ended in 2015, and all currently supported versions of Windows Server support SMB 2 or later.

### Client SMB connections

ONTAP enables SMB 1 support on SMB servers by default. SMB 1 cannot be disabled in ONTAP 9.1.

### Domain controller SMB connections

Beginning in ONTAP 9.1, SVMs can be configured to use specific SMB protocols (SMB 1 and SMB 2) when connecting to domain controllers. ONTAP 9.1 uses SMB 1 as the default SMB dialect for domain controllers.

```
vserver cifs security modify –vserver <vserver name> -smb1-enabled-for-dc-connections {true|false|system-default}
```

(default: system-default)

The system-default for ONTAP 9.1 domain controller SMB 1 connections is true.)

## 2.1 Planning for SMB Deprecation in ONTAP

SMB 1 support will be disabled by default in a future version of ONTAP. NetApp is following Microsoft’s lead in this regard because Microsoft has announced that it is deprecating SMB 1 and will be disabling it, by default, in a future version of Windows Server.

Customers should migrate to a more recent version of SMB as soon as possible.

Consider using `statistics show -object smb1` to audit your shares for SMB 1 traffic in order to determine if any of your clients are still using SMB 1.

## 2.2 Infinite Volumes

Infinite Volumes, containers that group storage resources across multiple aggregates and nodes into a single namespace optimized for scale and ease of management, are only compatible with SMB 1. Infinite Volumes are not compatible with SMB 2 or later.

Consider using FlexGroups to replace Infinite Volumes.

# 3 SMB 2

First available in Windows Server 2008 and Windows Vista, SMB 2 was a major rewrite of the SMB protocol, modernizing the protocol and bringing many enhancements—including simplified commands, asynchronous and compound operations, and increased read/write sizes—that resulted in significant performance improvements over SMB 1.

In addition to the performance gains, SMB 2’s durable handles and signing with HMAC-SHA256 are of particular importance to ONTAP.

### Client SMB connections

ONTAP enables SMB 2 support on SMB servers by default. To disable (or reenable) SMB 2, run:

```
vserver cifs options modify –vserver <vserver name> -smb2-enabled
{true|false}
```

(default: true)

(Advanced privilege level required.)

`-smb2-enabled` enables/disables both SMB 2 and SMB 2.1.

### Domain controller SMB connections

Beginning in ONTAP 9.1, SVMs can be configured to connect to domain controllers using SMB 2. ONTAP 9.1 uses SMB 1 as the default SMB dialect for domain controllers.

```
vserver cifs security modify –vserver <vserver name> -smb2-enabled-for-dc-
connections {true|false|system-default}
```

(default: system-default)

The system-default for ONTAP 9.1 domain controller SMB 2 connections is false.)

## 3.1 Durable Handles

SMB 1 is unable to prevent lock state from being lost during network outages. SMB 2 addresses this need with durable handles: file handles that are preserved by the client and can be used to reestablish disconnected sessions.

**Note:** Although durable handles are nondisruptive for volume moves and LIF migrations, they are not mirrored across nodes, and a failover (or an upgrade) of a node results in the lock state being lost. SMB 3’s persistent handles improve upon SMB 2 durable handles by mirroring lock state across nodes in a cluster.

### Details

When an SMB 2 client opens a file and establishes a lock, a durable handle is created that records session details, most importantly, the server that is associated with it. If the session is interrupted, the file remains open on the client, and the durable handle is used to reconnect the session.

**Note:** Durable handles are passive and require the client to reestablish disconnected sessions. The durable handle is lost if a client does not reestablish the session within 15 minutes.

You can view which files are using durable handles by using the `vserver locks show` command.

**Note:** When using `vserver locks show`, you can add additional parameters to display information about a smaller subset of existing locks. Parameters include:

- -vserver vserver_name
- -volume volume_name
- -path
- -lif
- -lockid

Durable handles are labeled as SMB Open Type: durable.

### Implementation

Durable handles are enabled by default.

**Minimum Requirements**

SMB 2

Vista, Windows Server 2008, or later

### Best Practices

LIF migrations can be used to balance or optimize network traffic across the cluster by moving network resources to storage resources.

When a LIF is migrated between nodes, client sessions become disconnected, but SMB 2+ clients using durable handles are able to reestablish the sessions and maintain nondisruptive operations.

## 3.2 SMB Signing

By default, SMB session traffic is not signed. This leaves it vulnerable to man-in-the-middle attacks, where attackers intercept traffic between the server and the client, modify it, and then forward it to the client.

To prevent SMB traffic from being intercepted on the network, customers can require that SMB signing be used to “sign” SMB data. SMB signing prevents the transmission and reception of data across a network from being altered by any method by authenticating that it comes from a trusted source and has not been tampered with.

### Details

Support for SMB signing is enabled by default in SMB 2, but is not required. When required, signing must be enabled by both the client application and the SMB share.

SMB 2 uses the HMAC-SHA-256 algorithm to sign packets and assure their authenticity.

SMB 3 uses AES-128-CMAC.

**Note:** SMB 1 uses the MD5 algorithm which is considered cryptographically broken and unsuitable for further use.

### Implementation

By default, SMB signing is not required by ONTAP. Use `-is-signing-required true` to require SMB signing at the SVM level:

- **SVM**

```
vserver cifs security modify -vserver <svm> -is-signing-required true
<true|false>
```

(default: false)

**Note:** Requiring SMB signing at the SVM level requires that all clients connecting to any shares on the client support SMB signing. Clients that do not support SMB signing are prevented from communicating with the SVM.

SVMDR relationships replicate SMB signing properties to the destination SVM if `identity-preserve` is set to `true`.

**Minimum Requirements**

- SMB 2
- Vista, Windows Server 2008, or later

### Best Practices

When an SMB session is signed, SMB communications experience increased CPU usage and performance degradation due to hash calculations. This has a negative impact on performance for both clients and servers.

Performance degradation associated with SMB is significantly less than that associated with SMB encryption, but should still be verified through testing in your specific network environment.

NetApp recommends using SMB signing on SVMs where security is essential to your organization.

**Note:** SMB signing may interfere with some solutions that by design (for example, WAN accelerators) act as a man in the middle and modify SMB network traffic.

## 3.3 SMB 2 Unsupported Features

### SMB Symbolic Links

Symbolic links (symlinks) are files that point to other files or directories. ONTAP does not support NTFS SMB symbolic links.

**Note:** ONTAP supports NTFS junction points and path mapping to NFS symlinks and widelinks. See the CIFS Reference Guide for more information about how to map symbolic links to Windows file shares and SMB clients.

### SMB Credit Pipeline

ONTAP does not support the SMB credit pipeline as a mechanism for controlling bandwidth by throttling client requests.

Instead, ONTAP grants clients as many credits as they request. Instead of using per-session credit limits, ONTAP can, if needed, implement SMB throttling by controlling the total number of requests from all clients.

# 4 SMB 2.1

First available in Windows Server 2008 R2 and Windows 7, SMB 2.1 brought improvements to the SMB protocol, including lease oplocks and large MTU support.

ONTAP enables SMB 2.1 support on SMB servers by default. To disable (or reenable) SMB 2.1, run:

```
vserver cifs options modify –vserver <vserver name> -smb2-enabled
{true|false}
```

(default: true)

(Advanced privilege level required.)

`-smb2-enabled` enables/disables both SMB 2 and SMB 2.1.

## 4.1 Lease Oplocks

Lease oplocks (opportunistic locks) serve the same client-side read-ahead, write-behind, and lock state caching purposes as traditional oplocks but provide additional flexibility and opportunities for reducing network traffic and increasing performance.

Significantly, lease oplocks allow multiple handles to be cached by a single client and multiple clients to cache a single file handle without breaking the lock.

### Details

Lease oplocks allow a client to obtain and preserve client caching state by generating a lease key and using it to link together multiple handles to the same file. ONTAP tracks the state using a client ID: a combination of the client's GUID and the lease key.

Lease oplock information can be viewed using the `vserver locks show` command.

**Note:** When using `vserver locks show`, you can add additional parameters to display information about a smaller subset of existing locks. Parameters include:

- -vserver vserver_name
- -volume volume_name

- -path
- -lif
- -lockid

### Implementation

Support for lease oplocks is enabled on SMB shares and volumes by default.

**Minimum Requirements**

- SMB 2.1
- Windows 7, Windows Server 2008 R2, or later

### Best Practices

Lease oplocks are essential for nondisruptive SMB operations in ONTAP. NetApp recommends that you do not disable them.

On the extremely rare chance that you must use ONTAP 9 to support a legacy database application that experiences significant performance degradation due to incompatibility issues with oplocks, oplocks can be disabled using:

```
vserver share properties remove -vserver vserver_name -share-name share_name
-shareproperties oplocks
```

**Note:** Disabling oplocks disables both traditional and lease oplocks. Disabling oplocks on a share takes precedence over the volume oplock setting.

### Breaking Locks

Oplocks require SMB clients to play nicely. If clients don't, you may need to step in to help.

A common example of a client not playing nicely is when it fails to release a lock and causes other clients to time out or experience access denied errors.

Should this happen, you can view currently held locks, identify the lock that is not being released, and break it manually.

Use `vserver locks show` (using additional parameters to fine tune your search) in order to display a list of currently held locks. Make note of the problem client's lock UUID. This is the lock you need to break manually.

To manually break the lock, use:

```
vserver locks break -lockid UUID
```

(Advanced privilege level required.)

## 4.2 Large MTU

Large MTU allows SMB's maximum transmission unit (MTU) to be increased from 64KB to 1MB, significantly improving the speed and efficiency of large file transfers by reducing the number of packets that need to be processed.

**Note:** Large MTU refers to large read/writes allowed by SMB 2.1 and later servers. It does not refer to MTU sizes by the network layer.

### Details

Client-server relationships that support large I/O sizes can drive higher throughput by reducing the number of transactions between the client and the server. By using fewer transactions, large MTU transmissions reduce network overhead.

### Implementation

By default, ONTAP uses small MTU and advertises max read and write sizes as 64K.

Large MTU can be enabled by using:

```
cifs options modify -is-large-mtu-enabled true
```

(default: false)

(Advanced privilege level required.)

**Minimum Requirements**

- SMB 2.1
- Windows 7, Windows Server 2008 R2, or later

### Best Practices

Copying large files (greater than 1GB) is dramatically improved by enabling large MTU, particularly by customers using high-bandwidth networks such as 10 Gigabit Ethernet or greater.

**Note:** Applications using small MTU (<64k) may see latency increases of ~1ms when operating in mixed-workload environments: for example, one in which many small MTU (<64k I/O) applications are running at the same time as many large MTU (1MB I/O) applications.

If mixed-workload latency increases are identified as a problem, NetApp recommends separating large and small writes into different aggregates.

## 4.3 SMB 2.1 Unsupported Features

### Resilient Handles

ONTAP does not support resilient handles. In many respects, resilient handles were an early step toward persistent handles. ONTAP supports durable (SMB 2) and persistent (SMB 3) handles.

# 5 SMB 3

First available in Windows Server 2012 and Windows 8, SMB 3 was a major improvement to the SMB protocol and saw significant enhancements such as scale-out, transparent failover, persistent handles, and witness that were designed to support continuously available shares on scale-out application file servers.

ONTAP enables SMB 3 support on SMB servers by default. To disable (or reenable) SMB 3, run:

```
vserver cifs options modify –vserver <vserver name> -smb3-enabled
{true|false}
```

(default: true)

(Advanced privilege level required.)

## 5.1 Continuous Available Shares

Continuous availability (CA) is a share property that, through the use of SMB scale-out, persistent handles, witness, and transparent failover, allows file shares to be accessible during otherwise disruptive scenarios such as controller upgrades or failures.

SMB CA shares are an essential requirement for SMB SOFS.

### Details

CA file shares mirror data, including lock state using persistent handles, across high-availability (HA) pair partners. If either partner experiences a failover (or upgrade) event, the partner node takes over and reestablishes SMB sessions using transparent failover. This reconnection happens so quickly that it is nondisruptive to SMB 3 clients.

Failures across nodes are disruptive for non-CA shares.

**Note:** Clients that do not support SMB 3 can connect and access data on a file share that has the continuously available property set, but are not able to take advantage of persistent handles and transparent failover.

### Implementation

NetApp supports CA shares for both Hyper-V over SMB and SQL over SMB use cases. Each use case has unique dependencies and configuration requirements that have been documented here:

- TR-4172: Hyper-V over SMB
- TR-4247: SQL Server over SMB

CA shares can be enabled by using:

```
-share-properties continuously-available
```

**Minimum Requirements**

- SMB 3
- Windows 8, Windows Server 2012, or later

### Best Practices

#### Nondisruptive Operations

CA shares are persistent across HA failover and giveback events. Hyper-V and SQL environments with this configuration are nondisruptive when upgrading to new versions of ONTAP because SMB sessions do not need to be terminated before starting the upgrade.

#### Unsupported Features

Home directory, change notify, attribute caching, BranchCache, access-based enumerations (ABEs), and automatic node referrals are not supported when using CA shares in ONTAP.

#### Unsupported Environments

Due to performance issues, CA shares should not be used with workloads that create large amounts of metadata. Performance for workloads associated with traditional file shares is much better in non-SOFS environments.

ONTAP does not support CA shares for use cases other than Hyper-V over SMB and SQL over SMB.

## 5.2 Scale-Out

SMB scale-out leverages functionality in SMB 3 to replicate data at the file share across nodes in a cluster.

SMB scale-out is an essential requirement for continuously available shares.

### Details

SMB scale-out uses cluster shared volumes (CSV) to provide simultaneous file share access across all nodes in a clustered file server. ONTAP is scale-out by design, and features such as SMB scale-out allow SMB 3 to provide better utilization of network bandwidth and load balancing than SMB 2.

**Note:** ONTAP does not currently support scale-out automatic load balancing. Scale-out load balancing is how SMB clients get automatic node referral-like performance gains on scale-out CA shares.

Unlike node referrals, which are location based, scale-out load balancing is performance based and allows clients to be routed to the share on the node with the lowest latency, taking advantage of the continuously available clustered architecture rather than hitting a bottleneck that might be present on a single high-traffic node.

### Implementation

ONTAP automatically enables support for SMB scale-out.

**Note:** SMB 2 clients can connect and access data on scale-out file shares but cannot take advantage of SMB 3 functionality.

SMB 1 clients cannot connect to scale-out file shares. Attempts to do so result in access denied error messages.

**Minimum Requirements**

- SMB 3
- Windows 8, Windows Server 2012, or later

## 5.3 Transparent Failover

Transparent failover allows SMB 3 clients to rapidly establish connections with continuously available shares on partner nodes. Transparent failover is a feature that, combined with scale-out, persistent handles, and witness, allows files shares to be made continuously available.

### Details

In ONTAP, if either partner of an HA pair experiences a failover (or upgrade) event, the partner node takes over. CA shares reestablish SMB sessions using transparent failover. This reconnection happens so quickly that it is nondisruptive to SMB 3 clients.

Failures across nodes are disruptive for non-CA shares.

**Note:** Clients that do not support SMB 3 can connect and access data on a file share that has the continuously available property set, but are not able to take advantage of transparent failover.

### Implementation

Transparent failover is enabled by default and an essential requirement for continuously available shares.

**Note:** ONTAP does not support transparent failover for use cases other than Hyper-V over SMB and SQL over SMB.

**Minimum Requirements**

- SMB 3
- Windows 8, Windows Server 2012, or later

## 5.4 Witness

If a non-CA share fails, SMB clients need to wait for an SMB or network timeout (usually between 30 and 300 seconds) before the session is considered lost.

On a CA share, witness provides rapid and nondisruptive operations by notifying SMB 3 clients that a session has been lost and redirecting them to a replicated CA share on another node in the cluster where the session can be reestablished using transparent failover.

### Details

Witness works by using remote procedure calls (RPCs) instead of waiting for Transmission Control Protocol (TCP) system calls.

When an SMB 3 client connects to a CA share, witness informs the client where it can find the same data in replicated CA shares on other nodes. The SMB 3 client registers this information, and, should a failure occur, rather than waiting for a network timeout to occur, witness notifies the client of the failure and initiates a transparent failover to quickly establish a new session on the alternate node.

### Implementation

Witness is enabled by default and an essential requirement for continuously available shares.

**Note:** ONTAP does not support witness for use cases other than Hyper-V over SMB and SQL over SMB.

**Minimum Requirements**

- SMB 3
- Windows 8, Windows Server 2012, or later

### Best Practices

Witness is highly dependent on SVMs and CA shares being correctly configured, including these requirements:

- At least one data LIF should be created per node for every SVM in the cluster.
- Automatic node referrals should be set to false.
- CA shares must be mapped by using NetBIOS or the fully qualified domain name.

Refer to Continuously Available Shares for specific details because each use case (Hyper-V over SMB and SQL over SMB) has unique dependencies and configuration requirements.

## 5.5 Persistent Handles

Although durable handles are nondisruptive for LIF and volume moves, they are not mirrored across nodes, and a failover (or an upgrade) of a node results in the lock state being lost.

Persistent handles improve upon SMB 2 durable handles by mirroring lock state across nodes in a cluster.

### Details

When an SMB 3 client opens a file and requests a persistent handle, additional information is provided to the SMB server (handle and resume key) that is shared between nodes in the cluster.

In case of a node failure or an upgrade, the persistent handle is preserved, while witness and transparent failover functionality connects the SMB client to an alternate node. As soon as the client has been verified using the resume key information in the handle, a session is established, and the client reclaims the file on the partner node.

Even though a new session has been established on a new node, lock state is preserved, and the operation is nondisruptive to the client.

You can view which files are using persistent handles by using the `vserver locks show` command.

**Note:** When using `vserver locks show`, you can add additional parameters to display information about a smaller subset of existing locks. Parameters include:

- -vserver vserver_name
- -volume volume_name
- -path
- -lif
- -lockid

Persistent handles are labeled as SMB open type: persistent.

### Implementation

Persistent handles are enabled by default and an essential requirement for continuously available shares.

**Note:** ONTAP does not support persistent handles for use cases other than Hyper-V over SMB and SQL over SMB.

**Minimum Requirements**

- SMB 3
- Windows 8, Windows Server 2012, or later

## 5.6 AES-128-CCM Encryption

AES-128-CCM replaced HMAC-SHA256 as the hash algorithm used by SMB encryption in SMB 3.

**Note:** AES-128-GCM has replaced AES-128-CCM in SMB 3.1.1.

### Details

By default, SMB session traffic is not encrypted. Sealing encrypts the data, a requirement for many applications. This includes user credentials such as names and passwords, which may be transmitted in clear text if not encrypted.

SMB encryption encrypts session traffic while it is in flight. It does not encrypt data at rest.

Unlike other encryption methods that maintain and/or manage a set of keys, key management is handled by the protocol using SMB encryption. It’s a self-contained security mechanism, and no additional key management is required.

### Implementation

SMB encryption can be enabled in ONTAP at the SVM or the share level using:

- **SVM**

  ```
  vserver cifs security modify –vserver <SVM> -is-smb-encryption-
  required <true|false>
  (default: false)
  ```

- **Share**

  ```
  vserver cifs share properties add –vserver <svm> -share-name <share> -
  share-property encrypt-data
  ```

**Note:** Enabling SMB encryption at the SVM level requires that all clients connecting to any shares on the client support SMB encryption. Clients that do not support SMB encryption or that support a specific SMB version’s encryption algorithm are prevented from communicating with the SVM.

**Minimum Requirements**

- SMB 3
- Windows 8, Windows Server 2012, or later

### Best Practices

When an SMB session is encrypted, all SMB communications to and from Windows clients experience increased CPU usage and performance degradation, affecting both the clients and the server (the nodes on the cluster running the SVM containing the file server).

Performance degradation associated with SMB encryption can vary widely and should be verified through testing in your specific network environment.

NetApp recommends using SMB encryption at the share level and only when in-flight data security is a requirement.

This recommendation:

- Allows clients that don’t support SMB encryption to still connect to shares that don’t contain information that needs to be secured while in flight.
- Provides flexibility in enabling the feature on an as-needed basis for only the data access points (that is, shares) that are necessary.

**AES-NI:** ONTAP 9 supports accelerated AES-NI encryption, which uses hardware acceleration to significantly improve the speed and efficiency of AES encryption and decryption over SMB, reducing performance degradation and CPU performance.

**Scale-out file servers**: CA shares using Hyper-V or SQL over SMB have latency dependencies that may not tolerate an increase in latency when using SMB encryption.

### 5.7 SMB 3 Unsupported Features

#### Directory Leasing

#### Multichannel

#### SMB Direct

## 6 SMB 3.1.1

First available in Windows Server 2016 and Windows 10, SMB 3.1.1 adds AES-GCM encryption, preauthentication integrity (the signing to encryption sealing), and enhancements to cluster client failover to the SMB protocol.

ONTAP enables SMB 3.1.1 support on SMB servers by default. To disable (or reenable) SMB 3.1.1, run:

```
vserver cifs options modify -vserver <vserver name> -smb31-enabled
{true|false}
```

(default: true)

(Advanced privilege level required.)

### 6.1 Preauthentication Integrity

By default, SMB session traffic is not signed. This leaves it vulnerable to man-in-the-middle attacks, where attackers intercept traffic between the server and the client, modify it, and then forward it to the client.

To prevent SMB traffic from being intercepted on the network, data can be signed in order to make sure that it comes from a trusted source and has not been tampered with.

Preauthentication integrity provides a similar function to that of SMB signing, but instead of signing every packet in an SMB session, preauthentication integrity only signs the client-server negotiate and session setup requests.

#### Details

SMB servers using earlier versions of SMB should be expected to generate NOT_SUPPORTED or INVALID_DEVICE_REQUEST status message errors because they are unfamiliar with preauthentication integrity. That’s expected—and OK—provided they respond to negotiate and session setup requests with a signed response.

### Implementation

Unlike SMB signing, which is optional, preauthentication integrity is required for all SMB 3.1.1 session traffic.

**Note:** Anonymous/null users or guest sessions cannot benefit from preauthentication integrity because they do not support SMB signing.

**Minimum Requirements**

- SMB 3.1.1
- Windows 10, Windows Server 2016, or later

### Best Practices

#### WAN Accelerators

Preauthentication integrity may interfere with solutions, for example, WAN accelerators, that rely on modifying SMB network traffic.

## 6.2 AES-128-GCM Encryption

AES-128-GCM replaced AES-128-CCM as the hash algorithm used by SMB encryption in SMB 3.1.1.

Importantly, GCM encryption is significantly faster (approximately 1.7x faster) than CCM encryption, making cost/benefit decisions in terms of increased security for decreased read/write performance easier than ever before.

SMB 3.1.1’s AES-128-GCM encryption is supported in ONTAP 9.1 and later releases.

### Details

By default, SMB session traffic is not encrypted. Sealing encrypts the data, a requirement for many applications. This includes user credentials such as names and passwords, which may be transmitted in clear text if not encrypted.

SMB encryption encrypts session traffic while it is in flight. It does not encrypt data at rest.

Unlike other encryption methods that maintain and/or manage a set of keys, key management is handled by the protocol using SMB encryption. It’s a self-contained security mechanism, and no additional key management is required.

### Implementation

SMB encryption can be enabled in ONTAP at the SVM or the share level using:

- **SVM**

```
vserver cifs security modify –vserver <SVM> -is-smb-encryption-
required <true|false>
(default: false)
```

- **Share**

```
vserver cifs share properties add –vserver <svm> -share-name <share> -
share-property encrypt-data
```

**Note:** Enabling SMB encryption at the SVM level requires that all clients connecting to any shares on the client support SMB encryption. Clients that do not support SMB encryption or that support a specific SMB version's encryption algorithm are prevented from communicating with the SVM.

**Minimum Requirements**

- SMB 3.1.1
- Windows 10, Windows Server 2016, or later

### Best Practices

When an SMB session is encrypted, all SMB communications to and from Windows clients experience increased CPU usage and performance degradation, affecting both the clients and the server (the nodes on the cluster running the SVM containing the file server).

Performance degradation associated with SMB encryption can vary widely and should be verified through testing in your specific network environment.

NetApp recommends using SMB encryption at the share level and only when in-flight data security is a requirement.

This recommendation:

- Allows clients that don't support SMB encryption to still connect to shares that don't contain information that needs to be secured while in flight.
- Provides flexibility in enabling the feature on an as-needed basis for only the data access points (that is, shares) that are necessary.

**AES-NI:** ONTAP 9 supports accelerated AES-NI encryption, which uses hardware acceleration to significantly improve the speed and efficiency of AES encryption and decryption over SMB, reducing performance degradation and CPU performance.

**Scale-out file servers**: CA shares using Hyper-V or SQL over SMB have latency dependencies that may not tolerate an increase in latency when using SMB encryption.

## 6.3 SMB 3.1.1 Unsupported Features

### Cluster Dialect Fencing

Cluster dialect fencing solves a multi-SMB dialect problem that doesn't exist in ONTAP.

Instead of dialect fencing, ONTAP uses capability management controls that prevent SMB functionality from being used until all nodes can take advantage of it.

NetApp recommends keeping the amount of time an ONTAP cluster needs to run different versions of SMB (and ONTAP) across nodes as short as possible. Batch upgrades can significantly reduce the time needed to accomplish multinode upgrades.

# Additional Resources

- CIFS Reference
  https://library.netapp.com/ecm/ecm_download_file/ECMLP2494081
- TR-4191: Best Practices Guide for Clustered Data ONTAP 8.2x and 8.3x Windows File Services
  http://www.netapp.com/us/media/tr-4191.pdf
- TR-4100: Nondisruptive Operations and SMB File Shares for Clustered Data ONTAP
  http://www.netapp.com/us/media/tr-4100.pdf

## Contact Us

Let us know how we can improve this technical report.

Contact us at docfeedback@netapp.com.

Include TECHNICAL REPORT TR-4543 in the subject line.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

### Copyright Information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

### Trademark Information