



Technical FAQ

SMB Technical FAQ

ONTAP 9.x

John Lantz, NetApp
Version 9.1
October 2016

Abstract

This technical FAQ is meant to assist NetApp SEs, PSEs, Support, and partners by providing answers to frequently asked questions surrounding the use and implementation of SMB/CIFS in ONTAP®. Topics include requirements, architecture, configuration, performance, and interoperability.

Information Classification

NetApp Confidential

Version History

Version	Date	Document Version History
Version 9.1.0	October 2016	John Lantz Added SMB 1, AES-GCM encryption, and offline files
Version 9.0.1	July 2016	John Lantz Added ODX and non-unicode device QA pairs.
Version 9.0	June 2016	John Lantz FAQ renamed to SMB technical FAQ. Updated for ONTAP 9. Questions recategorized as requirements, architecture, configuration, performance, or interoperability. 7-Mode questions relegated to 8.3 version.
Version 8.3.1	June 2015	Marc Waldrop Clustered Data ONTAP 8.3.1. Includes differences between 7-Mode and clustered Data ONTAP. CIFS Technical FAQ

TABLE OF CONTENTS

Version History	1
1 Overview.....	5
2 Requirements.....	5
Which version of SMB does ONTAP 9 support?	5
Which version of Windows supports which version of SMB?.....	5
Which version of SMB supports which features?.....	6
When will SMB 1 be deprecated?.....	6
Do I need Active Directory to deploy a CIFS server?	7
Does the time set on the ONTAP storage controller need to match the Active Directory domain time in order for a CIFS server created on a storage virtual machine (SVM) to join the domain?.....	7
Does ONTAP 9 support non-Unicode clients?.....	7
3 Architecture.....	7
How is access to CIFS determined?.....	7
How can I check to see if CIFS is licensed?.....	7
How can I verify that a CIFS server exists?	7
How can I verify that the right SMB version is enabled?.....	7
How can I verify that SMB is allowed for the SVM?	8
How can I verify that SMB is allowed on the network interface?.....	8
What is a namespace, and how does it relate to SMB?	8
What is a volume junction?.....	8
What are export policies, and do I need one?	8
What is the maximum character length supported for a path in CIFS?.....	8
Why does a folder show up as owned by BUILTIN\Administrators, yet the user who created it was domain\user3?.....	9
Is there a limit to the number of search paths that can be specified for home directories?	9
Can a share on a CIFS SVM house a distributed file system (DFS) root?	9
Which network ports might need to be reachable by a CIFS server?	9
What happens when a client attempts to map a drive to a share located on an ONTAP CIFS server?...	10
Does SMB encryption secure my data at rest?.....	10
Does ODX work on All Flash FAS (AFF) platforms?	10
4 Configuration	10
Should my CIFS server use the same name as the SVM on which it is installed?	10
I added a DNS CNAME entry to a CIFS server and can ping it CNAME but can't get access. What's wrong?.....	10
What happens if I set up a home directory that has the same name as an existing static share (for example, home directory john1) and an actual share named john1?.....	10
Can I set a group as the CIFS superuser?	11
What happens to file/folder permissions when I change the security style of a volume?.....	11
Does enabling SMB 3 enable SMB 3-capable client connections to survive storage events, including LIF migrate, ARL, and storage failover?	13

What does the symlink-properties option do when creating or modifying the particular setting on a CIFS share?	13
I need to enable a version of the SMB protocol in my SVM that was previously disabled (whether by default or manually disabled). Does it affect data access for existing clients?	13
I have folders in a share that one client can see but not another. It occurs on Windows 7 clients and later when using SMB 2 to connect.	13
Can I use automatic node rebalancing when using CA shares and Hyper-V?	14
Is it possible to control which LIF autolocation (node referral) refers a client?	14
I changed the path where my CIFS share points (referring to a new volume or qtree). However, the client still sees data from the old location.....	14
Does ONTAP support both modes of BranchCache (hosted cache and distributed cache)?	14
Is SMB 3 witness the same as file share witness in a Microsoft cluster?	14
5 Performance.....	14
Is there a performance impact to using SMB 3 encryption?	14
What is the difference between AES-GCM and AES-CCM SMB encryption?	15
What NetApp platforms support AES-NI?.....	15
Is there NDO for CIFS when activating a DR scenario when using SVMDR?	15
How do I view multiprotocol user mapping (that is, UNIX UIDs to NT SIDs) in ONTAP?	16
What does the “status” column information mean in the output of “cifs domain discovered-servers show”?	16
What is the end-user experience during a storage failover event?	17
6 Interoperability.....	18
Which Kerberos cypher does ONTAP 9 use?.....	18
What is the maximum Kerberos token size support for CIFS authentication?	18
Do I have to maintain separate encryption keys for SMB encryption?.....	18
Is LDAP TLS the same thing as LDAP signing and sealing?.....	18
Does ONTAP 9 support off-box antivirus?.....	18
What happens if I don't specify a security style for a FlexVol volume or a qtree during creation?.....	19
Do I need to have user mapping functioning if I am only going to use CIFS or NTFS security style volumes or qtrees?	19
I get an error that reads, “Error: Strong(er) authentication required,” when setting up CIFS. What am I doing wrong?	19
Does ONTAP 9 support LDAP over SSL?	19
Does NetApp support Microsoft's work folders feature?	19
Is the SMB share property “continuously available” supported for general information worker type workloads (that is, home directories or project shares)?	19
Can I use offline files (client-side caching) with CA shares?	19
Can I use Microsoft Management Console (MMC) to manage an ONTAP CIFS server?	20
Why are my offline files not working?	20
Additional Resources	21
Contact Us	22

1 Overview

ONTAP 9 brings new SMB/CIFS feature support to ONTAP, including SMB 3.0 accelerated AES-NI encryption, SMB 2.1 large MTU, and native auditing. Additionally, ONTAP 9 supports LDAP signing and sealing, workgroup authentication, null user, and IP qualifiers, all new to NetApp® clustered environments and bringing parity with the same features found in Data ONTAP® 7-Mode.

This technical FAQ is meant to assist NetApp SEs, PSEs, Support, and partners by providing answers to frequently asked questions surrounding the use and implementation of these and other SMB/CIFS features in ONTAP.

2 Requirements

Which version of SMB does ONTAP 9 support?

Answer: SMB 3.1.1 and earlier.

Which version of Windows supports which version of SMB?

Answer:

	SMB 1	SMB 2	SMB 2.1	SMB 3	SMB 3.02	SMB 3.1.1
Windows Server 2016 Windows 10	✓	✓	✓	✓	✓	✓
Windows Server 2012 R2 Windows 8.1	✓	✓	✓	✓	✓	✗
Windows Server 2012 Windows 8	✓	✓	✓	✓	✗	✗
Windows Server 2008 R2 Windows 7	✓	✓	✓	✗	✗	✗
Windows Server 2008 Windows Vista	✓	✓	✗	✗	✗	✗
Previous versions	✓	✗	✗	✗	✗	✗

Which version of SMB supports which features?

Answer:

SMB 2:

- Simplified commands
- Asynchronous operations
- Compound operations
- Durable handles
- Increased read and write size
- HMAC-SHA256

SMB 2.1:

- Lease oplocks
- Large MTU support
- BranchCache

SMB 3:

- Continuous availability
- Witness
- Persistent handles
- Scale-out file servers
- AES-CCM encryption
- VSS for SMB file shares
- ODX copy offload
- Transparent failover

SMB 3.1.1:

- AES-GCM encryption (ONTAP 9.1)
- Preauthentication integrity
- Cluster client failover (CCF) v2

When will SMB 1 be deprecated?

Answer: 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.

Use `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.

Do I need Active Directory to deploy a CIFS server?

Answer: No. When in workgroup mode, a CIFS server does not need Active Directory. Workgroup mode CIFS servers allow CIFS clients to authenticate to the server using locally defined users and groups.

Be aware that domain-based features are disabled in workgroup mode and cannot be used. (SMB 3 witness protocol, SMB 3 CA shares, SQL Server over SMB, folder redirection, roaming profiles, group policy objects, and volume snapshot service are not supported.)

Does the time set on the ONTAP storage controller need to match the Active Directory domain time in order for a CIFS server created on a storage virtual machine (SVM) to join the domain?

Answer: Yes, within five minutes. This requirement is for all servers joining an Active Directory domain. Set the time and the time zone, and set up Network Time Protocol (NTP) on the storage controller to point to the same time source server (or domain controller) that other domain member servers use to enable authentication. This requirement is a Microsoft requirement related to Kerberos.

Does ONTAP 9 support non-Unicode clients?

Answer: No. ONTAP 9 only supports Unicode clients when accessing data using SMB.

3 Architecture

How is access to CIFS determined?

Answer:

- Valid CIFS license
- CIFS server exists
- CIFS versions enabled
- CIFS allowed on the SVM
- CIFS allowed on the data LIF
- CIFS share exists
- Required permissions on the share exist
- Required permissions on the files and folders exist

How can I check to see if CIFS is licensed?

Answer:

```
license show -package CIFS
```

How can I verify that a CIFS server exists?

Answer:

```
cifs server show -vserver [SVM_name]
```

How can I verify that the right SMB version is enabled?

Answer:

```
cifs server options show -vserver <SVM_name> -fields smb2-enabled,smb3-enabled
```

How can I verify that SMB is allowed for the SVM?

Answer:

```
vserver show -vserver [SVM_name] -fields allowed-protocols
```

How can I verify that SMB is allowed on the network interface?

Answer:

```
network interface show -vserver [SVM_name] -fields data-protocol
```

If CIFS is not allowed on the data LIF, then the LIF must be destroyed and recreated, or a new LIF needs to be created. The ports allowed on a data LIF depend on the allowed data protocol. For example, if CIFS is not enabled on a data LIF, then ports 139 and 445 are not available in a LISTEN (listening for incoming connections) state.

What is a namespace, and how does it relate to SMB?

Answer: A namespace is a logical grouping of separate volumes joined together by junctions to create a single logical file system. It is logical in the sense that all the volumes may or may not be located on the same node. When a volume is created, junction paths can be used to organize into a single namespace.

When a share is created, it is tied to a path in the namespace. For example, a volume called foovol is mounted in ONTAP to /foovol. In order to access foovol, when a CIFS share is created, it needs to be pointed to /foovol.

Later, if you create goovol and mount it under /foovol/goovol in ONTAP, it is available to those users who have access to the share pointing to foovol. When you use the share to navigate to foovol, users see a folder call goovol. The junctions appear as an ordinary directory to a CIFS client.

What is a volume junction?

Answer: When you create a volume in ONTAP, a junction allows the volume to be mounted for later presentation using a CIFS share. A junction isn't required when you create a volume; however, a junction is necessary in order to make the volume available to CIFS clients.

What are export policies, and do I need one?

Answer: Export policies for CIFS are effectively a third level of security beyond your typical share- and file-level permissions. Export policies are optional and disabled by default for CIFS.

What is the maximum character length supported for a path in CIFS?

Answer: This is traditionally 255 characters and is not controlled by ONTAP. See "Naming Files, Paths, and Namespaces" in the MSDN for more information: <http://msdn.microsoft.com/en-us/library/aa365247.aspx>.

Why does a folder show up as owned by BUILTIN\Administrators, yet the user who created it was domain\user3?

Answer: The user domain\user3 was a member of the BUILTIN\Administrators group locally on the CIFS server. This membership is either direct or indirect using an associated group. This approach is used to match Microsoft behavior and is not NetApp specific.

Consider using group policies to control membership permissions instead of adding accounts as BUILTIN or domain admins, which enable more domain control to a user than is likely intended.

See [https://technet.microsoft.com/en-us/library/cc756898\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/cc756898(v=WS.10).aspx) for more information.

Is there a limit to the number of search paths that can be specified for home directories?

Answer: No. Keep in mind that if you configure home directories in ONTAP, a client request to connect to a home directory path is tried on all paths specified by the search path (in the order specified) until a matching folder is found. As the search path grows to include more volumes, users whose home directories reside near the end of the specified locations may see an impact on their workstation logins. The user's home directory is mapped as part of the user's standard Windows client login.

Can a share on a CIFS SVM house a distributed file system (DFS) root?

Answer: No. A share that is available on a CIFS SVM can be the target of a DFS link configured on a DFS server, but cannot house the DFS root.

Which network ports might need to be reachable by a CIFS server?

Answer:

Protocol	Destination Port	Source Port	Port Details
TCP/UDP	53	1024-65535	DNS
TCP/UDP	88	1024-65535	Kerberos
TCP	135	1024-65535	RPC
TCP/UDP	137	1024-65535	NetBIOS name server
UDP	138	1024-65535	NetBIOS datagram
TCP	139	1024-65535	NetBIOS session services
TCP/UDP	389	1024-65535	LDAP
TCP	445	1024-65535	SMB over TCP
TCP/UDP	464	1024-65535	Kpasswd

What happens when a client attempts to map a drive to a share located on an ONTAP CIFS server?

Answer:

1. The client begins with a three-way TCP handshake to ports 139 and 445.
2. The CIFS server generally responds to both three-way TCP handshake requests.
3. The client generally breaks down the connection to port 139.
4. The client and server exchange SMB “negotiate protocol” calls to determine the SMB version to use for the connection.
5. The client and server exchange SMB “session setup” calls in which, among other things, the user is authenticated (that is, the user name or Kerberos ticket is exchanged here).
6. The client and server exchange SMB “tree connect” calls in which the client passes to the server the name of the share to which it intends to connect.

Does SMB encryption secure my data at rest?

Answer: No. SMB encryption secures data in transit between source and destination.

Does ODX work on All Flash FAS (AFF) platforms?

Answer: Yes. ODX requires that compression be disabled, which has caused concern for AFF users given that AFF platforms enable inline compression by default.

To clarify, ODX requires that secondary compression be disabled. ODX works as normal with the adaptive, inline compression that is enabled by default on AFF platforms

4 Configuration

Should my CIFS server use the same name as the SVM on which it is installed?

Answer: No. The CIFS server name *can* match the SVM name, but to avoid confusion it *shouldn't* because an SVM can serve different purposes, including serving CIFS, NFS, iSCSI, and/or FCP clients and hosts. When accessing a CIFS share, you need to reference the CIFS server, not the SVM on which it lives.

I added a DNS CNAME entry to a CIFS server and can ping it CNAME but can't get access. What's wrong?

Answer: It's possible that the environment disabled NTLM authentication and allows only Kerberos. When you created the DNS CNAME, it allowed the client to get routed to the CIFS server using name resolution discovery. However, the client was unable to obtain a Kerberos ticket to authenticate. An SPN alias may resolve the issue. See the following NetApp Support KB article for more details: <https://kb.netapp.com/support/index?page=content&id=2018231>.

What happens if I set up a home directory that has the same name as an existing static share (for example, home directory johnl) and an actual share named johnl?

Answer: A user attempting to connect to the user's home directory share is directed to the static share. Home directory shares are “pseudo” shares that exist but are not created through a manual process. A static share is one created by an admin. When faced with a conflict like this, the client is connected to the static share and not the home directory. Verify that you don't have conflicts between pseudo shares that are created for a home directory and actual storage admin-defined shares.

Can I set a group as the CIFS superuser?

Answer: No, only a user.

What happens to file/folder permissions when I change the security style of a volume?

Answer: It depends on the security type you are changing to and from, along with the permissions on the data. The following are a few examples that show the impact of changing the volume security style.

Environment: Active Directory domain = domain all Windows users map to a user name that is equal to their UNIX account (example: Windows user Domain\user16 has an equivalent UNIX user name of User16).

ACL	Change from → To	Change to ACL After Style Change	Result
Everyone: read and execute Domain\user15: full control Domain\user14: full control Owner: Domain\user15	NTFS → UNIX	No	The resulting UNIX mode bit permissions would be 755. The NTFS ACL is converted to UNIX mode bits such that it doesn't provide any more access than would have been granted when the security style was NTFS. In this case, because Domain\user15 had full control, the "owner" bit is 7. The everyone group is what dictates the remainder of the mode bits. In this case the "group" and "other" bits are set to allow read and execute. In this case the user Domain\user14 loses the ability to write to the file.
Domain\user15: full control Domain\user14: full control Owner: Domain\user15	NTFS → UNIX	No	The resulting UNIX mode bits are 700. Again, the NTFS ACL is analyzed, and UNIX mode bit permissions are set to not allow any more permissions than would be allowed if it were still NTFS. In this situation, because there is no everyone group, the UNIX ACL cannot assign permissions for group and other. As a result, the only person who has access to the file is the UNIX user15. To restore access to other users, user15 needs to modify the UNIX ACL accordingly. ***See following copy for the impact that takes place when you change the permissions on files after a

			volume security style change.
--	--	--	-------------------------------

When you change the security style of a volume, the previous ACL is retained in the background. As long as there are no changes to the ACL for the file or directory, then the original ACL is retained in the background. For example:

File name: foo.txt
NTFS ACL: everyone: read and execute; domain\riggoj full control; domain\user14 full control
Security style change: NTFS → UNIX
After security style change, the UNIX ACL would show: 755 (everyone entry would limit access to group and other)
Make no changes and change the security style back: UNIX → NTFS
Postchange, NTFS ACL would show: everyone: read and execute; domain\user15: full control; domain\user14: full control

The key is that the ACL was not modified while set to UNIX. If in the preceding example a user from a UNIX workstation mounted an NFS export that points to the location where foo.txt resides and typed `chmod 775 foo.txt`, the original NTFS ACL would be gone. After switching the security style back to NTFS, permissions to the file would need to be modified to restore write access for domain\user14. To show the impact, here is the same scenario with the UNIX “chmod” inserted.

File name: foo.txt
NTFS ACL: everyone: read and execute; domain\user15 full control; domain\user14 full control
Security style change: NTFS → UNIX
After security style change, the UNIX ACL would show: 755 (everyone entry would limit access to group and other)
Issue the command “chmod” from UNIX user15: `chmod 757 foo.txt`
Change the security style back: UNIX → NTFS
Resultant NTFS ACL: domain\user15: full control, domain\user14: read and execute, all others: full control

In order to restore the Windows user domain\user14 access to “write” to the file, you need to re-ACL it using manual modification or set inheritance on a parent folder. The ACL, when viewed, contains entries that say something similar to “user (UNIXPermUId\user)” and/or “unixgroup (UNIXPerGid\unixgroup).” In order to either manually set the permissions or set inheritance, entries that contain the wording UNIX... need to be removed prior to attempting to set a new NTFS ACL; otherwise, it fails.

Does enabling SMB 3 enable SMB 3-capable client connections to survive storage events, including LIF migrate, ARL, and storage failover?

Answer: No. Enabling the SMB 3 protocol on an SVM does not make the connection capable of nondisruptive operations. In order to provide complete NDO for the SMB 3 protocol, you need to specify the share property as continuously available (CA). Continuously available shares are supported on SQL Server on Hyper-V workloads only.

What does the symlink-properties option do when creating or modifying the particular setting on a CIFS share?

Answer: This option controls whether symlink resolution for CIFS is enabled on a share. The setting is a per-share setting and has the following settings:

ONTAP 9 Symlink-Properties Options
Enable
Read_only,enable
Hide
"" (null) or "-"
Symlinks
Symlinks_and_widelinks
disable

The settings for symlink properties are important for multiple reasons. The first is it controls how symlinks are advertised and accessible to SMB clients (note that these are not NTFS symlinks, which are not supported). DFS advertisement is possible by specifying symlinks, symlinks_and_widelinks, or disabled.

Refer to KB "What is the impact of a shares symlink settings and DFS advertisement in clustered Data ONTAP on SMB 2.x/3 client traffic" for more information:

<https://kb.netapp.com/support/index?page=content&id=3014510>.

I need to enable a version of the SMB protocol in my SVM that was previously disabled (whether by default or manually disabled). Does it affect data access for existing clients?

Answer: No. Connected clients continue to use the protocol version negotiated with the ONTAP CIFS server during the initial connection. New connections that are established attempt to use the newly enabled SMB protocol versions depending on the client's capability. When clients attempt to initiate connections to a CIFS server, they present a list of SMB dialect versions they support. This is done through the negotiate protocol exchange. The server looks at the list and selects the highest version it supports and has enabled. Clients with an existing connection continue to work, and new clients can take advantage of the different protocol versions enabled.

I have folders in a share that one client can see but not another. It occurs on Windows 7 clients and later when using SMB 2 to connect.

Answer: This issue could very well be due to a client side introduced with the SMB 2 protocol. See the following article for Microsoft that explains the client-side caches and how to disable them:

<http://technet.microsoft.com/en-us/library/ff686200%28v=ws.10%29.aspx>.

Can I use automatic node rebalancing when using CA shares and Hyper-V?

Answer: No. Automatic node rebalancing is only supported for non-CA shares.

Note: ONTAP does not currently support scale-out rebalancing. (Performance based rebalancing rather than location-based rebalancing.) Scale-out node rebalancing provides node referral-like performance gains for scale-out CA shares. (SMB 3, WS 2012R2).

Is it possible to control which LIF autolocation (node referral) refers a client?

Answer: No. Autolocation works by looking at the SVM's data LIFs relevant to the location of the volume itself. If the data LIFs where the volume resides are assigned the NFS and CIFS protocols, then those LIFs are candidates for referral. If an interface is down but would normally meet the criteria for referral, it is not used. The interface needs to be in the up state and must also have both CIFS and NFS as allowed protocols.

I changed the path where my CIFS share points (referring to a new volume or qtree). However, the client still sees data from the old location.

Answer: If you change the path of the CIFS share to point to a new location and don't have your client disconnect and reconnect to the share, the client still references the old path. The reconnect is necessary due to the client tracking its connection using what's called a tree ID, or TID. The TID is provided during the initial connection to a CIFS share during the tree connect exchange. This ID is used to associate a client's connection to a share path.

Does ONTAP support both modes of BranchCache (hosted cache and distributed cache)?

Answer: Yes, but with the clear distinction that the SVM is only a content server in the BranchCache architecture. An SVM is not participating as a caching server in a BranchCache setup. BranchCache works off of identifiers that are based on hashes. The first client to request access to the data is the client who initially caches the data (in a distributed model) or who sends the data to a central server for caching (in a hosted model). The second, third, and later clients who access the same data are provided identifiers to locate the data on either its peers or a central caching server. For more details about BranchCache, see official Microsoft documentation about how the feature works and is architected.

Is SMB 3 witness the same as file share witness in a Microsoft cluster?

Answer: No. SMB 3 witness is a feature within SMB that allows faster failover of a SMB connection between an SMB 3 client and a server. A file share witness (FSW) in a Microsoft cluster is used to assist in establishing a quorum for Microsoft Windows clusters.

5 Performance

Is there a performance impact to using SMB 3 encryption?

Answer: Yes, and it can be a notable impact. The impact is similar to using SMB signing and could be higher. The impact is different because SMB signing is merely reading the data and computing a signature that is added to the frame. SMB encryption is reading the data and then writing it back out in a secure encrypted format, which results in additional CPU usage. The performance changes are seen in increased CPU despite the network traffic staying the same. The recommendation is to test using a workload that one expects to have when accessing data you intend to encrypt.

What is the difference between AES-GCM and AES-CCM SMB encryption?

Answer: 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.

What NetApp platforms support AES-NI?

Answer: ONTAP support for hardware-accelerated AES-NI encryption significantly improves the speed and efficiency of AES encryption and decryption over SMB, reducing performance degradation and CPU performance.

Hardware Universe, hwu.netapp.com, lists the chipset used by specific NetApp controllers. Chipsets supporting AES-NI are listed on the Intel ARK site, <http://ark.intel.com/search/advanced/?s=t&AESTech=true>

Is there NDO for CIFS when activating a DR scenario when using SVMDR?

Answer: No. There is a client interruption to data access when you activate the DR side in an SVMDR relationship. SVMDR is an asynchronous replication DR technology that uses SnapMirror® to replicate configuration details and user data. The SVMDR relationship makes sure that the configuration information between source SVM and destination SVM is replicated.

Note: When using ID-preserve, configuration between source and destination match. When using ID-discard CIFS domain, name resolution and network settings are not replicated.

SVMDR makes sure that user data is replicated from source SVM to the SVM in the DR cluster. However, no information about the current lock state for any open files is transferred over to the DR cluster. When activating the DR side in an actual DR scenario, the connected SMB clients prior to the DR scenario have to reestablish connection to their previously opened files. Again, this is an asynchronous DR technology between separate clusters.

How do I view multiprotocol user mapping (that is, UNIX UIDs to NT SIDs) in ONTAP?

Answer: The command is available from the diag-level CLI and is `diag secd authentication show-creds -node <nodeName> -vserver <SVMName> -win-name <domain\winUserName>`.

See <http://community.netapp.com/t5/Data-ONTAP-Discussions/What-is-the-right-command-to-show-me-user-mapping/td-p/106195>.

The following is an example of looking up a Windows user:

```
diag secd authentication show-creds -node RTPClus-01 -vserver cifs01 -
win-name RTPNC\bobbyj
```

```
UNIX UID: bobbyj <> Windows User: RTPNC\bobbyj (Domain User)
```

```
GID: nistestgroup
```

```
Supplementary GIDs: <None>
```

```
Windows Membership:
```

```
RTPNC\Domain Users (Domain group)
```

```
BUILTIN\Users (Alias)
```

```
User is also a member of Everyone, Authenticated Users, and Network
Users
```

```
Privileges (0x80)
```

What does the “status” column information mean in the output of “cifs domain discovered-servers show”?

Answer:

Status	Meaning
OK	The connection to this server is usable.
Unavailable	The server is currently unavailable for use.
Slow	The connection to the server is usable but has been determined to be slow.
Expired	The connection to this server expired.
Undetermined	This server has been discovered but has not been used.
Unreachable	This server was discovered but is no longer reachable.

What is the end-user experience during a storage failover event?

Answer: The answer depends on the protocol version that the client uses to connect to the storage controller. Depending on the protocol version running and the configuration of CIFS shares, during a storage failover event, the node that does the takeover might have no record of open files on the failing node. When a file is open over a CIFS share, the lock state for that file is held in memory. During an SFO event, the lock state is lost when the surviving node takes over. Depending on the version of the SMB protocol that the connection uses, it dictates the ability (or lack thereof) for the clients to survive an SFO event.

- **SMB 1**

SMB 1 has no way to recover any previously open file handles; the protocol just doesn't have this capability. The open file handles are held in memory, and thus when the controller fails over to its partner, the lock state for open files is not present. A client sees an interruption to open files/folders at the time of a failover event.

- **SMB 2**

SMB 2 introduced durable handles and an increased capability to survive some storage events. Durable handles allow brief network interruptions to occur between client and storage. During an SFO event, the client is disconnected from the controller while the LIF is migrated. After the LIF is migrated and brief network interruption resolved, a client attempts to reconnect to a previously opened file from the failed node. However, a downfall of durable handles is that they are not guaranteed to survive a reboot of either client or server. Despite the ability to survive the brief network disruption, the loss of the state of the file between storage cluster nodes is why SMB 2.x cannot survive an SFO event. Although they are a giant step forward for CIFS and resiliency, SMB 2.x have limitations. They do not survive server reboots, and multiuser access to the same file can cause the loss of durability because durable handles rely on certain oplock or lease levels to retain durability. In addition, durable handles are passive. A client needs to issue I/O against an open file so that the connection to the durable handle is maintained after a survivable event. Again, however, because lock state is kept in memory on the node where the file resides and because durable handles are designed for intermittent network drops versus full-scale reboots of hosts, the clients see a disruption in access to open files.

- **SMB 3-non-CA (noncontinuously available)**

SMB 3-non-CA acts like the SMB 2

- **SMB 3-CA (continuously available)**

Clients connecting to the storage controller using SMB 3 and shares that have the continuously available share property set can survive a storage failover event. Generally the clients see a slight pause in any active I/O that occurred at the time. The survivability is made possible by features such as persistent handles, witness, and lock mirroring that were introduced in SMB 3 and CA-capable shares/connections.

For more details about maintaining operational ability during storage events, consult TR-4100: Nondisruptive Operations and SMB File Shares.

6 Interoperability

Which Kerberos cypher does ONTAP 9 use?

Answer: ONTAP 9 supports AES-128-CCM (SMB 3) and AES-128-GCM (SMB 3.1.1).

What is the maximum Kerberos token size support for CIFS authentication?

Answer: ONTAP 9 supports Kerberos tokens up to 64k.

Do I have to maintain separate encryption keys for SMB encryption?

Answer: No. SMB encryption is self-contained, using keys based on HMAC-SHA256 (SMB 2), AES-CCM (SMB 3), and AES-GCM (SMB 3.1.1) algorithms, and is managed through the protocol itself.

SMB encryption can be enabled at the SVM or share level through separate options. The recommendation is to enable it on a per share basis due to the nature of mixed client versions in most environments. The feature is only supported by clients who support the SMB 3 protocol. If the feature is enabled at the SVM level, encryption needs to be negotiated for any share connection regardless of the per share setting (that is, the SVM setting supersedes the share setting).

Is LDAP TLS the same thing as LDAP signing and sealing?

Answer: No. The following few bullets show where they are similar and where they are not.

- **LDAP over TLS**

- Signs and seals all session traffic, securing the transmission of LDAP authentication information during the bind phase, particularly for those who use simple binds.
- Utilizes a certificate to accomplish the securing of data in transit.
- Requires that the communication to succeed over TLS or LDAP traffic is not exchanged.
- The connection to the LDAP server MUST use port 389. Configuration to any other port fails.

- **LDAP signing and sealing**

- Provides the option of signing, or signing and sealing, traffic between an SVM's CIFS server and LDAP clients.
- When LDAP signing is enabled, anonymous and simple binds are rejected.
- Signing data authenticates that the data comes from a trusted source and has not been tampered with, providing a good defense against man-in-the-middle attacks.
- Sealing encrypts 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.

Does ONTAP 9 support off-box antivirus?

Answer: Yes.

What happens if I don't specify a security style for a FlexVol volume or a qtree during creation?

Answer: The volume/qtree inherits a security style upon creation, depending on several factors. Those factors are:

- FlexVol® volumes inherit the security style of the root volume of the SVM where the FlexVol volumes are being created.
- Qtree inherits the security style of the parent FlexVol volume in which it is being created.
- The exception is Infinite Volumes; they always use the unified security style.

Do I need to have user mapping functioning if I am only going to use CIFS or NTFS security style volumes or qtrees?

Answer: Yes. All Windows users need to map to a UNIX user when connecting to shares, regardless of the security style.

I get an error that reads, "Error: Strong(er) authentication required," when setting up CIFS. What am I doing wrong?

Answer: This error message indicates that communication with the domain controller has a higher requirement for LDAP connections than has been enabled. Enable LDAP signing and sealing as required.

Does ONTAP 9 support LDAP over SSL?

Answer: No. NetApp ONTAP 9 does not support LDAP over SSL because of known security issues that deprecated the protocol. SSL is considered insecure.

ONTAP 9 supports LDAP over TLS. If an LDAP server has any of the TLS protocols enabled (that is, TLSv1, TLSv1.1, or TLSv1.2), no further action is required. For customers upgrading to ONTAP 9, at least one of the TLS protocols must be enabled at the server to make sure of connectivity.

Does NetApp support Microsoft's work folders feature?

Answer: No. Work folders require the use of locally attached storage. The lack of support is not a NetApp limitation but rather how Microsoft implemented the feature.

Is the SMB share property "continuously available" supported for general information worker type workloads (that is, home directories or project shares)?

Answer: No. The continuously available share property is only supported for SMB connections for Hyper-V servers and SQL Server 2012. General information worker (using CIFS shares for project data or home directory storage) is not supported. Microsoft provides similar guidance on general information work and CA shares.

Can I use offline files (client-side caching) with CA shares?

Answer: Yes, although NetApp and Microsoft recommend that you do not.

This answer changes to no in Windows 10, as Microsoft has removed the capability to use offline files with CA shares in Windows 10. Please refer to:

<https://blogs.technet.microsoft.com/filecab/2016/03/15/offline-files-and-continuous-availability-the-monstrous-union-you-should-not-consecrate/>

Can I use Microsoft Management Console (MMC) to manage an ONTAP CIFS server?

Answer: Yes and no. You can manage the following: create/delete CIFS shares, manage open files, and manage client sessions.

When using MMC to manage open files and client sessions, the view of those is node specific. This means that when you use MMC and add in the computer management snap-in specifying the CIFS server as the computer to which you want to connect, if you use an FQDN or short name, then when the connection is made, DNS is consulted to resolve the name. On whichever cluster node the connection is made, the display of sessions and open files is what that node knows.

Consider this example: an SVM has four nodes, and each has a data LIF. Each data LIF is registered in DNS to serve traffic for a CIFS server named CIFS01. When you specify in the computer management snap-in the host name CIFS01, DNS is consulted, and the management workstation connects to one of four nodes. Let's say all the open files and sessions are on node 4 of the cluster, but the snap-in connects to node 1. When viewing the open files and session, the MMC shows nothing or just the session established by the admin workstation. In order to see all the open files and sessions, you need to add another computer management snap-in and specify the IP address associated with the data LIF that resides on node 4.

The other alternative would be to use the ONTAP PowerShell Toolkit, version 3.2 or later, which contains cmdlets that provide a clusterwide enumeration of open files and sessions. The cmdlets are `get-nccifssession`, `get-nccifssessionfile`, `close-nccifssession`, and `close-nccifssessionfile`.

Why are my offline files not working?

Answer: Because Offline Files (client-side caching/CSC) also need to sync data from other (not currently logged on) users on the computer, the Offline File sync does not exclusively take place in the rights context of the logged on user.

Offline Files require a set of minimum permissions to be able to sync correctly. Not setting the permissions correctly on the file server will cause sync problems and can prevent the client from switching to online mode.

Minimum permissions for the share, the NTFS permissions of the shared folder and the permissions for each folder in the path are documented in: <http://support.microsoft.com/kb/2512089/en-us>.

Note: Microsoft does not recommend using offline files with CA shares and has removed the capability to do so on CA shares in Windows 10.

Additional Resources

- Top 10 CIFS issues and solutions in ONTAP.
<https://kb.netapp.com/support/index?page=content&id=3014312>
- CIFS Reference Guide
https://library.netapp.com/ecm/ecm_download_file/ECMLP2494081
- CIFS and NFS Auditing Guide
https://library.netapp.com/ecm/ecm_download_file/ECMLP2494084
- CIFS/SMB Configuration Express Guide
https://library.netapp.com/ecm/ecm_download_file/ECMLP2495118
- SMB SE Technical Presentation
<https://fieldportal.netapp.com/content/437325>
- TR-4543: SMB Protocol Best Practices
www.netapp.com/us/media/tr-4543.pdf
- TR-4100: Nondisruptive Operations and SMB File Shares
www.netapp.com/us/media/tr-4100.pdf
- TR-4191: Windows File Services Best Practices
www.netapp.com/us/media/tr-4191.pdf
- TR-4189: CIFS Auditing Quick Start Guide
www.netapp.com/us/media/tr-4189.pdf
- TR-4247: Deploying SQL Server 2012 over SMB 3 CA Shares
www.netapp.com/us/media/tr-4247.pdf
- TR-4449: FPolicy Solution Guide for Clustered Data ONTAP: Peer Software PeerLink
www.netapp.com/us/media/tr-4449.pdf
- TR-4479: FPolicy Solution Guide for Clustered Data ONTAP: Northern Storage Suite (NSS)
www.netapp.com/us/media/tr-4479.pdf

Contact Us

Do you have a question that you think we should include in this FAQ?

Ask us at docfeedback@netapp.com.

Include SMB TECHNICAL FAQ 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.

Copyright Information

Copyright © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Fitness, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANshare, SANtricity, SecureShare, Simplicity, Simulate ONTAP, SnapCenter, SnapCopy, Snap Creator, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, StorageGRID, Tech OnTap, Unbound Cloud, WAFL, and other names are trademarks or registered trademarks of NetApp Inc., in the United States and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.