**HOST END ERRORS & TROUBLESHOOTING**

**Error:**

**Cifs “slowness”, or inability to write files to a NAS destination. Or developer is reporting “access denied” errors**

Solution:

Have Windows platform check share and file level permissions.

If cifs share is on a unix style qtree have Unix platform make sure permissions are wide open – chmod 777 (as they control security).

You can also check CIFS latency in the NMC, but also insure mandatory scanning is OFF

**Error:**

**“Permission denied” when Unix tries to mount**

Solution:

Verify exports. Hosts for volumes in vfilers must have static routes.Also, make sure a pipe (|) doesn’t appear in the exports (so two host entries appear as one)

**Error:**

**CIFS Server not joined to domain**

Solution:

Correct the HOST(A) record within DNS, using the netbios name of the CIFS server.

Verify that the Windows user has the ability to add or modify permission from windows security tab

**Error:**

**Failed to apply Cifs local users and groups from 7mode to Cdot**

Solution:

Ping DNS Server. If ping fails reacding to domain controller and finding SID fails, Run manual translate reqest to SID in diag mode,Run authentication tranlate request to know domain names,If ping to DNS is successful, there may be port blockage. Run Packet trace

**Error:**

**CIFS clients are unable to access any CIFS shares of a CIFS server**

Solution:

Create the CIFS server computer account in Active Directory

Reset the CIFS server password

Delete and recreate the CIFS server

Note: Deleting the CIFS server will not delete the data but will delete all the CIFS shares previously created

**Error:**

**CIFS: Cannot view the Security tab from Windows client**

Cause

The following are a few possible causes:

User account does not have proper permissions to access the Security tab.

File/folder contains UNIX security permissions, not NTFS ACLs.

User is not a member of the administrator group that is able to set Audit Security Information on the file/folder

DACL policy is applied to the SVM and the user does not have access to set Audit Security Information via the DACL.

Solution

To determine why the user account does not have the appropriate access, run the commands:

::>vserver security file-directory show

::>vserver security trace

::>vserver security file-directory ntfs dacl show

**Error:**

**Unable to access CIFS shares**

Cause

When the number of sessions allowed per user over a TCP connection is exceeded.

Further session establishment requests are denied until sessions are released.

This is typically caused by a misbehaving client or application not closing sessions.

Solution

Investigate misbehaving client or application and close stale sessions.

**Error:**

**Client unable to access CIFS shares: Many simultaneous new CIFS connections**

Issue

CIFS client is unable to access CIFS shares, while access from some clients is still possible

Cause

By design, once 256 NTLM authentication requests occurred and haven't completed within the same TCP session, ONTAP will reject any further authentication requests.

This is likely a process from the problematic client not answering the NTLM CHALLENGE as expected or not closing its connections.

Solution

Investigate and correct the client behavior

Close the TCP connection

Connect to the share using a different DNS alias from the client, which will create a new TCP session

**Error:**

**No client access to CIFS in takeover**

Issue

Client access to CIFS is lost during takeover.

Cause

One of DNS server IP addresses has been mistyped during the initial DNS configuration.

Solution

Check SECD logs and DNS configuration and correct accordingly.

**Error:**

**Unable to access recently created CIFS shares**

Issue

Unable to access any recently created CIFS shares, but able to access older CIFS shares.

Cause

SnapMirror relationship has been quiesced/suspended so volumes/shares created after the suspension weren't synced to SnapMirror destination.

When user tries to access a volume/share that was created after the suspension, the new volume/share is not found resulting in cifsShrConnectFailed error.

Solution

Resume SnapMirror with command:

cluster2::> snapmirror resume -destination-path snapmirror\_destination\_path

The snapmirror resume command must be used from the destination vserver or cluster

**Error:**

**Unable to mount volume using CIFS on Linux client and fails with Error "Host is Down"**

Issue

Host is Down error observed while mounting SMB share on Linux client.

Cause

SMB1 is disabled on the CIFS server

Solution​

Enable SMB1 on the CIFS server

OR

Use SMB version 2.0/3.0 on Linux client

**Error:**

**Troubleshooting CIFS Latency - Single volume readdir workloads with high latency**

Solution:

The Primary and most optimal solution is to enable CIFS Home Directory feature. This would help to dramatically reduce the number of SMB calls.

One solution might be to move workload off or split workload across more nodes for 7-Mode or more volumes\nodes in C-MODE.

If there are many "stale" user home folders, moving or deleting these will help reduce the number of directories being enumerated.

Flexgroup configuration could also be deployed in C-MODE environments.

Disable other CIFS features such as Access Based Enumeration (ABE). This could allow for more CPU headroom to service READDIR workloads.

If a large directory is suspected, see this article on how to locate a large directory.

It is best to limit number of users to 10,000 or less if using FlexVols, and create more FlexVols as needed.

**Error:**

**CIFS shares not displaying in Windows Explorer**

Cause

Cause 1)

If you are receiving on of the following errors or if you can see the shares when browsing via ip address but not by name, this may be an authentication failure:

Error 1:

Windows cannot access \\<servername >

Error 2:

Logon failure: unknown user name or bad password

Error 3:

An authentication error has occurred. The Local Security Authority cannot be contacted.

This could be due to an expired password. Please update your password if it has expired.

Cause 2)

This may be caused by a duplicate IP address. To verify, look in the EMS logs for the following message:

netinet.ethr.duplct.ipAdrr:error]: Duplicate IP address 10.1.1.2 sent from Ethernet address: ff:ff:ff:ff:ff:ff.

Cause 3)

Browsing of the shares may be turned off on the share (although the default for each share is configured as browsable). To verify, run the command:

::> vserver cifs share show -vserver <vserver>

Look under "properties" to see if the relevant share is browsable.

Solution

Solution 1)

The Troubleshooting Authentication Failures KB will further assist with resolving these issues.

Solution 2)

Change the IP address on either the vserver's LIF, or the host with the duplicate IP address.

Solution 3)

Add the "browsable" share property with the following command:

::> cifs share properties add -vserver <vserver> -share-name <share\_name> -share-properties browsable

**Error:**

**CIFS Disconnects from Windows host with error "Too many creds on single session"**

Cause

The CIFS session from the application server was blocked because it was interpreted as a DOS attack on the cluster after excessive session setup requests. The cluster will only allow 255 pending SMB session setup requests before it interprets the connect as an attack to overwhelm the cluster. This is by design to protect the cluster and is a hard coded limit that cannot be modified.

A packet trace will show multiple session setup requests in the same stream until it hits this limit. In a type All ASUP, the SKTLOGD will show this behavior.

Solution

This behavior has been addressed in later software versions, as documented in bug 932514. If upgrading to a fixed version is not available, the connection can be reset from either filer or the client as a temporary fix:

From Data ONTAP:

identify the connection using the command:

vserver cifs session show -session-id >65000 -fields connection-id,node

terminate the connection using the command:

network connections active delete -node <node> -cid <connection-id>

From client:

restart the host or CIFS

remap the CIFS share

For clustered systems, failover may also work as a temporary solution to this problem. For clients that encounter this issue frequently, SMB1 can be used as a workaround by disabling SMB2.

**Error:**

**CIFS access denied errors in ONTAP 9 after enabling SMB encryption**

Issue

After enabling "-is-smb-encryption-required" CIFS security option, some clients are no longer able to access CIFS shares.

The issue impacts clients running Windows versions earlier than 8 or Server 2012, while newer clients are still able to access shares.

In trace, we're seeing "STATUS\_ACCESS\_DENIED" being returned to Session Setup Requests.

Cause

End-to-end encryption is only supported by SMB 3 and above

SMB 3 is not supported prior to Windows 8 or Windows Server 2012

Mandatory encryption requirement cannot be met over SMB 2, so access to the share is denied

Solution

There are two possible workarounds:

Upgrade clients to OS versions supporting SMB 3

Disable mandatory encryption

vserver cifs security modify -is-smb-encryption-required false

**Error:**

**Cannot access CIFS shares if SVM root volumes is offline**

Issue

CIFS\SMB shares visible in Windows but not accessible. A client may terurn "an internal error occurred."

New NFS mounts to the same location may also be impacted

EMS messages may also report:

Nblade.CifsOperationTimedOut: Detected a timed out CIFS operation. SMB command for this operation:

Cause

The root volume of the CIFS SVM has been taken offline

Solution

Bring the root volume online to recover CIFS share access

**STORAGE END ERRORS & TROUBLESHOOTING**

**Error:**

**Troubleshooting Workflow: DC not responding (CIFS) DC/DNS Not Responding**

Cause

The causes and procedures to be performed to resolve this issue are described in the Solution section below.

Note: The causes and solutions are the same for both DC or DNS being unreachable.

Cause 1: Time skew; error message when using Kerberos check the secd.log

Resolution:

If the time on the client, DC, and/or Cluster (node) are outside of the configured clock skew, then Kerberos will not work as per the default settings in AD.

Cause 2: Machine password is out of sync; error message using Kerberos despite correct time

Resolution:

::> cifs password-reset -vserver vserver

Cause 3: Machine account is deleted in the Active Directory

Resolution:

Create a machine account with the CIFS server name in the Active Directory.

Cause 4: Using a DNS alias/CNAME, without the SPN set for that alias

Resolution:

If using a DNS alias/CNAME, the SPN should be added for that alias to ensure Kerberos is being used.

Cause 5: Using a DNS alias/CNAME for which the SPN is set, but for a different account

Resolution:

If the above machine account is not the intended machine account, delete the SPN for that machine account.

**Error:**

**What is the impact of modifying/deleting or recreating a cifs server on ONTAP?**

Answer

Q1: What is the impact of running CIFS setup again (7-mode)?

Cifs setup cannot be run until the CIFS service is terminated.

CIFS Setup can not be run while CIFS is active

The "cifs terminate" command will cause the cifs service to be stopped for the particular vfiler it is run against.

When cifs is terminated, the symlinks, shares, and share acl’s will remain intact.

Q2: What is the impact of running CIFS create again?

Running cifs create a second time requires that the cifs server be deleted. See question 3 below for impact of deleting a cifs server.

Q3: What is the impact of deleting and recreating a CIFS server?

Any current smb\cifs sessions will be closed. New smb\cifs authentication will be denied until the cifs server is created again.

Cifs symlinks/widelinks configuration will be deleted for the vserver

Cifs shares and share acls for the vserver will be deleted. .

Data contained in the shares will not be deleted

Cifs server/security options may be deleted.

Q4: What is the impact of modifying a CIFS server name?

Modifying the cifs server name requires that the cifs service on the vserver to be set to administratively down (closing all cifs connections)

Q5: What is the impact of modify the domain of a CIFS server?

Modifying the domain of the cifs server requires that the cifs service on the vserver be set to administratively down (closing all cifs connections).

Q6: What is the impact of modifying the organizational unit (OU) of a CIFS server?

Modifying the OU of the cifs server requires that the cifs service on the vserver be set to administratively down (closing all cifs connections).

**Error:**

**Vfiler is not pingable**

Solution:

Run vfiler status –r. If the vfiler says “unconfigured” (below in red), go into the NMC, vfiler units | select vfiler in question | setup | check box for “change network settings” | see if interface says “none”, if it does select the correct interface (e.g. change from none to correct interface (e.g. corpvif0-2502), and proceed through wizard and click finish | wait a bit and then try to ping. (you might have to select the correct template, network too (corp) etc…)

**Error:**

**Error received when trying to run cifs setup on a vfiler: (text of error approximate)**

**“vfiler is currently being run on this system so the command timed out after 60 seconds.  The command will continue to try to run and may succeed later.”**

Solution:

Vfilers can only have one administrative command running at a time (serial not parallel). This can be as simple as dfm already running a stats gathering command, etc. You need to simply verify that your command completed and/or try again.

**Error:**

**Could not reuse existing volume(s) in dataset node or selecting a new aggregate for provisioning a volume.**

Solution:

Add aggregates into the resource pool.Or also, check the protocols for the vfiler (add the NFS protocol if missing)

**Error:**

**It appears you don’t have any resource pools.**

Solution:

Checking CIFS as an available protocol if a CIFS license is not installed will make it appear as if you do not have any resource pools.

**Error:**

**Lifs are not pinging**

Solution:

**Make sure the IP address has LIF associated with it.**

Make sure the LIF status-admin is up

Make sure the LIF is operationally up.

Make sure the configuration is correct.

**Error:**

**What are the CIFS statistics to be collected for individual user sessions?**

Answer

When a storage system or a controller is running Data ONTAP 8.x for CIFS. The administrator can collect the ops, reads, writes, ios and suspicious stats. The storage system with cifs.per\_client\_stats.enable option on collects statistics on a per-client basis. This allows the use of the cifs top command, as well as the -uand-h options of CIFS stat for vfilers.

Note: Administrators must be aware that there will be an overhead when collecting the per-client stats.

The overhead might noticeably affect the storage system performance. If the options are turned off, any existing per-client statistics are discarded.

The cifs.per\_client\_stats.enableoption is turned offby default.

Default: off

Effective: Upon CIFS client reconnection

Persistence: Remains in effect across system reboots

Usage:

cifs top [-n <maxclients>] [-v] [-s <sort>] [-a <avg>]

<sort> is {ops|reads|writes|ios|suspicious}.

<avg> is {smooth|now|total}.

Above two can be abbreviated and default to first choice.

Usage:

cifs stat [-v[v]] [-h <ip-or-host>] [-u <user>] [ <interval> ]

cifs stat [-z]

cifs stat [-c]

-v, -h and -u only available when the options "cifs.per\_client\_stats.enable" is on.

-h option only available in vfiler context.

-u option only available in vfiler context.

Example

user1-2> cifs top

ops/s reads(n, KB/s) writes(n, KB/s) suspect/s IP Name

0 | 0 0 | 0 0 | 0 | 10.63.97.34 NETAPPuser1