NetApp Knowledge Base

How to troubleshoot CIFS share and export policy access permissions

https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_OS/How_to_trou…

Updated: Wed, 31 Aug 2022 14:27:42 GMT

Applies to

ONTAP 9

Description

- Check the following basic items before troubleshooting further:
  - Connectivity to the Domain is functional and the time between the SVM, Domain Controller and clients are in sync
  - The SVM is running
  - CIFS is licensed and running on the SVM
  - The CIFS Protocol is enabled on data LIFs

Procedure

- Complete the following steps.

1.Confirm share path and permissions

- Check if the desired path is shared from the SVM, by running the cifs share show command
- In the below example, verify the path /files is shared, and verify the ACL entry to which it is shared to

```
cluster::> cifs share show -vserver svm1

Vserver        Share         Path              Properties Comment
 ACL
-------------- ------------- ----------------- ----------
-------- -----------
svm1           admin$        /                 browsable  -
 -
svm1           c$            /                 oplocks    -
 BUILTIN\Administrators / Full Control
                                                browsable
                                                changenotify
                                                show-previous-
versions
svm1           ipc$          /                 browsable  -
 -
3 entries were displayed.
```

- In the above example, it is seen that the path /files are shared as "Public" to the "Everyone" group with "Full Control" permissions
- Make sure that the user you are trying to validate has access to this share is a member of the group "Everyone"

The default share-level ACL is Everyone Full Control

2. Check to see if the export policy is enabled on the SVM for CIFS

- It is highly possible that an export policy exists, but is not enabled for CIFS. On later versions of ONTAP, the default for the SVM is to have an export policy created but, not enabled for CIFS
- Run the `cifs options show` command at the advanced privilege level to see if the export policy is enabled for CIFS
- In the below example (after going to the advanced privilege level), you can see that Vserver svm1

has export polices enabled for CIFS

```
cluster::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use
them only when directed to do so by NetApp personnel.Do you want
to continue? {y|n}: y

cluster::*> cifs options show -vserver svm1 -fields is-
exportpolicy-enabled
vserver  is-exportpolicy-enabled
-------      ------------------------------
svm1      true
```

If export policies are not enabled for the CIFS SVM, proceed to the next section

3. Check for the existence of an export policy on the vserver
   - Typically export policies are used to control access to folders and files for NFS clients. However, they can also be used to restrict access to CIFS folder and files as well. Run the vserver export-policy show command to see if an export policy exists.
   - In the below example, you are looking to see if the veserver svm1 has any policy's applied.

```
cluster::*> vserver export-policy show -vserver svm1

Vserver          Policy Name
---------------  -------------------
svm1             default
```

If export policies are not enabled for the CIFS SVM, proceed to the next section

4. If an export policy exists and is enabled for CIFS, you must check to see if this policy has a rule which can restrict access to the CIFS share path
   - Run the vserver export-policy rule show command to examine all of the rules that exist within the export policy
   - In the below example, it is seen that the rule could be applying to the user that is attempting to access the CIFS share because the protocol is set to "cifs”

```
cluster::*> vserver export-policy rule show -vserver
svm1
Vserver
Policyname          Ruleindex    Access   Clientmatch Protocol
 ROrule RWrule   anon  superuser
```

```
------------ --------------- ------  --------
--------------------- ---------
svm1    default             1            any      0.0.0.0/
0    cifs      never never    65534 none
```

- In this case, the first rule is preventing access to the file or folder due to the read only rule and read write being set to 'never'
- To test that an export policy rule might be causing an issue, a simple test would be to create a wide-open export policy rule and assigning volume files to it

```
cluster::*> export-policy create -vserver svm1 -policyname
wide_open


cluster::*> export-policy rule create -vserver svm1 -policyname
wide_open -clientmatch 0.0.0.0/0 -protocol any -rorule any
-rwrule any -superuser any


cluster::*> vol modify -vserver svm1 -volume files -policy
wide_open

Volume modify successful on volume file of Vserver svm1
```

If the export policy rules are verified and not preventing access, continue to the next section

5. If you determine that an export policy is preventing CIFS access to the file or folder then you need to delete that export rule
   - Make sure that the rule is not providing access to other client types (like NFS) before you delete the rule
   - Run the vserver export-policy rule delete command to remove the export rule that is preventing CIFS access
   - In the below example, we are deleting the 1st rule in the default policy that we noted was set to 'never' for RO and RW in the Step 4 above

```
cluster::*> vserver export-policy rule delete -vserver svm1
-policyname default -ruleindex 1

Warning: The last rule in the export-policy "default" is being
deleted. All volumes and qtrees using this policy will become
inaccessible.
Do you want to continue? y
```

Additional Information

N/A