NetApp® Knowledge Base

"Access denied by server while mounting" with NFS Kerberos

Applies to

- ONTAP 9

Issue

When issuing a mount command from an NFS client in an environment leveraging Kerberos, you may encounter the following error:

```
mount.nfs: access denied by server while mounting
```

Cause

This is potentially caused by missing or incorrect SPNs for LIF(s) associated with the NFS server's machine account.

Solution

Add the appropriate SPNs to the NFS server's machine account.

Additional Information

- **How a client builds an SPN**
    - Mounting using IP:
        - Client queries DNS for reverse lookup of IP
        - DNS returns name associated with the IP
        - Client uses this name to construct the SPN
    - Mounting using name:
        - Client uses name from the mount command to construct the SPN
- **Kerberos During the NFS Mount Process**

When an NFS client mounts through Kerberos, the following process takes place:

- DNS is queried for the hostname/IP lookup. The DNS name is used to formulate the NFS SPN request.
- The NFS client SPN is used to perform an Authentication Service request (AS-REQ) from the KDC.
- If the NFS client SPN exists on the KDC and the password/keytab authentication succeeds, then a Ticket Granting Service request (TGS-REQ) is initiated from the client for the NFS SPN.
- The NFS client's SPN is used in a krb-unix name mapping operation in ONTAP. If the Kerberos SPN can map to a valid UNIX user, then the mount request is allowed. If there is no valid name mapping,access is denied.
- The NFS server export-policy rules are checked to make sure that client access is allowed. If access is allowed to that client through NFS Kerberos, then the mount succeeds. If the export-policy rules do not have that client or allow Kerberos in the rules, access is denied.

NOTE :

- Read access should be allowed to the root volume of the SVM (vsroot) to NFS clients when a rule is assigned.

- If the export policy restricts read access to the vsroot will cause denial in traversal to the volumes created under that SVM and cause mounts to fail.
- That is because vsroot is "/" in the path to "/junction" and factors into the ability to mount and traverse.

Refer NFS Kerberos in ONTAP (section 1.5 discusses SPNs in greater detail.) Also refer page 47 for other Common Issues