NetApp Knowledge Base

After migration, CIFS is inaccessible using DNS name (IP address works)

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

Updated: Fri, 20 Nov 2020 07:37:51 GMT

Applies to

ONTAP 9

Issue

- A migration from a different storage system (such as a Data ONTAP 7-Mode controller) is complete and the DNS A record is modified so that the original name maps to a IP address of a CIFS SVM data LIF
- On attempting to access the CIFS server using `\\CIFSSVM` there is a hang and timeout followed by a generic network path not found error
- Ping or nslookup of the DNS name is successful and using the IP address works
- Logging on and off, clearing DNS cache, or rebooting the client does not help

'NetApp provides no representations or warranties regarding the accuracy or 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 customers responsibility and depends on the customers ability to evaluate and integrate them into the customers operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.'

1

Cause

- Kerberos authentication is failing due a conflict in the Microsoft Service Principal Names (SPN) configuration. DNS is configured to direct traffic to the new CDOT SVM AD object, however this SPN is in use by the original AD object. The DC sees this as identity spoofing and prevents the connection, causing authentication to fail.
- Using the IP address works because NTLM authentication is used. In order to authenticate with Kerberos, a valid SPN must be used to access the CIFS server. By default, an AD object is configured with a SPN that matches the name of the object, so a DNS record with the same name must be used.

Solution

- A possible quick workaround is to remove the original storage system AD computer object. Removing it will prevent the original CIFS server from functioning alongside the CIFS SVM. This will resolve the SPN DNS name and SPN mismatch, however it will still not allow Kerberos authentication to succeed. When using a DNS name that is not configured as an SPN, Kerberos authentication will still fail and the client will fall back to NTLM authentication if it is enabled.
- To follow best practices, Kerberos authentication should be used because it is more secure and quicker than NTLM (older standard still for legacy). The short (netbios or single label) name and the Fully Qualifiy Domain Name (FQDN) that will be used to access the new CDOT SVM should be added as SPNs.
- SPNs are attributes of AD objects and can be added by using the Microsoft 'setspn.exe' utility (built into modern versions of Microsoft Windows operating systems). Minimum permissions to read and modify AD objects is required, which is normally granted to domain administrators by default.

1. List to the SPNs set for the the original storage system and new CDOT SVM AD computer object:

```
C:\> setspn -l FILERA
C:\> setspn -l SVM1
```

- Only the HOST/ SPNs are required. CIFS/ and NFS/ or other SPNs can be ignored.
- The SVM AD computer object might be different than expected. You can find what it is by running the below command in the cluster CLI:

```
cluster::> vserver cifs show -fields cifs-server,ou
```

2. Delete the SPNs from the original AD computer object that os being decommissioned:

```
C:\> setspn -d HOST/FILER1 FILER1
C:\> setspn -d HOST/FILER1.domain.com FILER1
```

- You can also remove the AD object to delete all SPNs associated with it. This will make the original CIFS server inaccessible.

3. Add the SPNs to the CDOT SVM AD computer object:

```
C:\> setspn -s HOST/FILER1 SVM1
C:\> setspn -s HOST/FILER1.domain.com SVM1
```

- If you still require the original storage system to be accessible with Kerberos authentication, add different SPNs to it. You can also run 'cifs setup' on 7MODE to create a new machine account AD object and this will automatically have the SPNs set that match the machine account name chosen.

```
C:\> setspn -s HOST/FILER1old FILER1
C:\> setspn -s HOST/FILER1old.domain.com FILER1
```

- Allow AD replication to complete. If a user was logged on and attempted to access the SVM, they will need to log off and on. New users will be able to log on and access the SVM normally. Depending on the environment and applications, a reboot of the client may be required. If that is not possible, Microsoft has utilities to manually clear the cache.

Additional Information

additionalInformation_text