

SMB Access Fails When Using a DNS Alias



Table of Contents

- 1. Symptom 1
- 2. Cause 1
- 3. Resolution 1
 - 3.1. Install the PowerShell Active Directory Module 1
 - 3.2. Find and Remove the Existing Service Principal Names 2
 - 3.3. Add Them to the Cluster's Computer Object 2

Applies to: Hammerspace 5.2 and later.

1. Symptom

Clients can reach a share by its NetBIOS name or its fully qualified domain name, but not by a DNS alias (a CNAME record). The clients are running Windows 10, Windows 11, Windows Server 2016, or later.

Typical errors:

```
\\cluster-vanity-name.hammerspace.com\share_name is not accessible:  
You might not have permission to use this network resource.
```

```
Account restriction is preventing this user from signing in.
```

```
Logon Failure: The target account name is incorrect.
```

2. Cause

Kerberos needs a service principal name matching the name the client used. When clients reach a share through a DNS alias or NetBIOS name, the matching service principal names have to exist on the cluster's Active Directory computer object.

Two are needed for each alias:

- HOST/alias
- HOST/alias.domain

For an alias of `hr.domain.com`, that means `HOST/hr` and `HOST/hr.domain.com`.

A service principal name can only belong to one computer object at a time. If the alias was previously used by the source NAS, its service principal names are still on that object, and adding them to the cluster fails until they are removed.

3. Resolution

Find any existing alias service principal names on the source NAS computer object, delete them, then create them on the cluster's computer object.

3.1. Install the PowerShell Active Directory Module

On a Windows machine joined to the same domain as the cluster, open PowerShell as administrator:

Command:

```
Install-WindowsFeature RSAT-AD-PowerShell
```

3.2. Find and Remove the Existing Service Principal Names



Do not remove the HOST service principal names that match the source NAS computer object's own name — that can stop clients reaching the NAS. To free those, rename the NAS itself, which renames its computer object. See your vendor's documentation.

Find them, replacing `alias_fqdn` with the alias:

Command:

```
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

Delete the ones you want to move, replacing `alias_fqdn` with the alias and `file_system_dns_name` with the source NAS DNS name:

Command:

```
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')[0].Name.Split(".")[0]
$SourceAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
SetSPN /D ("HOST/" + ${Alias}) ${SourceAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${SourceAdComputer}.Name
```

Repeat for each alias you are moving.

3.3. Add Them to the Cluster's Computer Object

Replace `file_system_dns_name` with the cluster's SMB server name, which you can find in the GUI at **Administration > Active Directory** in the **SMB Server Name** field. Replace `alias_fqdn` with the alias.

Command:

```
$HSDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $HSDnsName | Where Type -eq 'A')[0].Name.Split(".")[0]
$HSAdComputer = (Get-AdComputer -Identity $FileSystemHost)
```

```
Set-AdComputer -Identity $HSAdComputer -Add @"msDS-AdditionalDnsHostname" = @($Alias, $Alias.Split(".")[0])
```

Verify both service principal names are present:

Command:

```
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')[0].Name.Split(".")[0]
$HSAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
SetSpn /L ${HSAdComputer}.Name
```

Repeat for each alias. Clients can now reach shares over SMB using those aliases.