

Shares Are Inaccessible After Upgrading Domain Controllers to Windows Server 2022



Table of Contents

1. Symptom	1
2. Cause	1
3. Resolution	2

Applies to: Hammerspace 5.2 and later.

1. Symptom

After Active Directory domain controllers are upgraded to Windows Server 2022, clients can no longer reach shares using an alias DNS entry or an IP address.

In the example used here, the cluster's Active Directory computer object is `jv-hs-a.asgard.local`, and clients reach the cluster either through a DNS alias of `file.asgard.local` or through the IP address `192.168.10.10`.

2. Cause

Windows Server 2022 changed how NTLM authentication is handled, and Microsoft has announced plans to deprecate NTLM entirely.

Those changes break authentication when a client connection falls back from Kerberos to NTLM – which happens when the computer object has no HOST service principal name matching the DNS name or IP address the client used.

Joining the cluster to the domain creates two HOST service principal names automatically, both based on the computer object name: one for the single-label hostname, one for the fully qualified domain name.

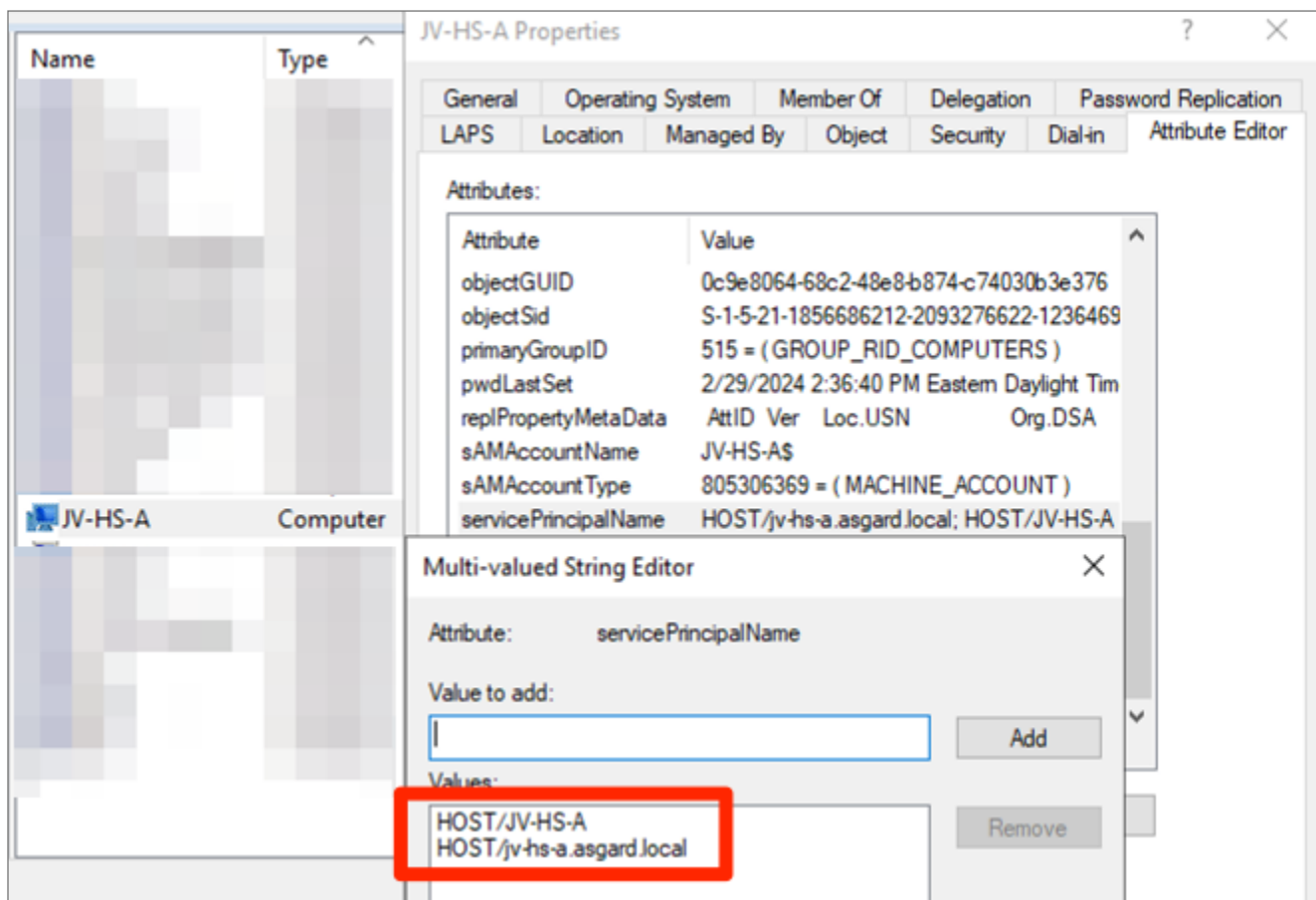


Figure 1. The two HOST service principal names created by default

A client reaching the cluster by any other name — a different DNS record, or an IP address — fails Kerberos and falls back to NTLM. Before Windows Server 2022 that fallback succeeded. Now it is rejected.

3. Resolution

Create HOST service principal names for every name and IP address clients use to reach the cluster, including both the single-label and fully qualified DNS entries. Kerberos can then be used throughout, and nothing falls back to NTLM.

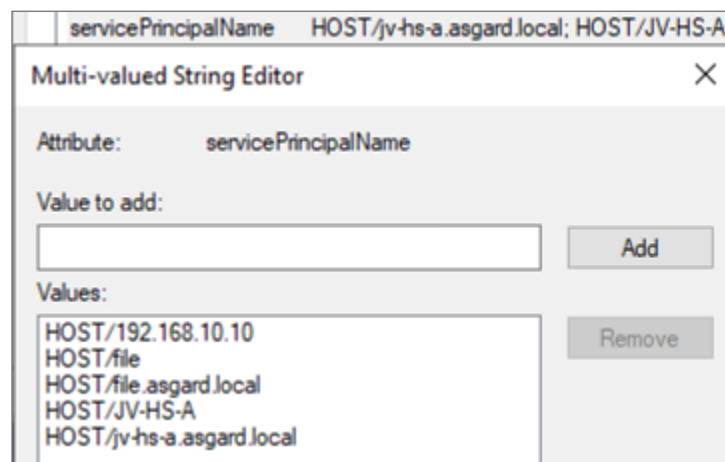


Figure 2. The computer object with the additional service principal names added



- Service principal names must be unique within the domain, as computer object names are.
- Active Directory will not let you reuse a HOST service principal name within the same domain.
- Add every service principal name the cluster needs at deployment, even where NTLM still works in your environment.