MIRAGE

Report

Topic	Incident Report – Missing DNS Record for nats-svc
Writer	Network Infrastructure Team (IT Team)
Date	May 6, 2025

Summary

On May 3, 2025, the Development team reported they were unable to resolve the hostname **nats-svc.mirage.htb**. This hostname is critical for internal service communication with the NATS messaging system hosted on the Mirage domain.

Timeline of Events:

- **May 3, 2025**: The nats-svc server becomes unreachable within the internal network.
- **May 4, 2025**: The Development team reports a failure to connect to the NATS service via DNS.
- **May 5, 2025**: An initial investigation confirms the DNS record for nats-svc is missing from the **mirage.htb** zone.

Research / Findings:

When the Development team attempted to connect to the NATS server using the nats-svc hostname, they received a connection error :

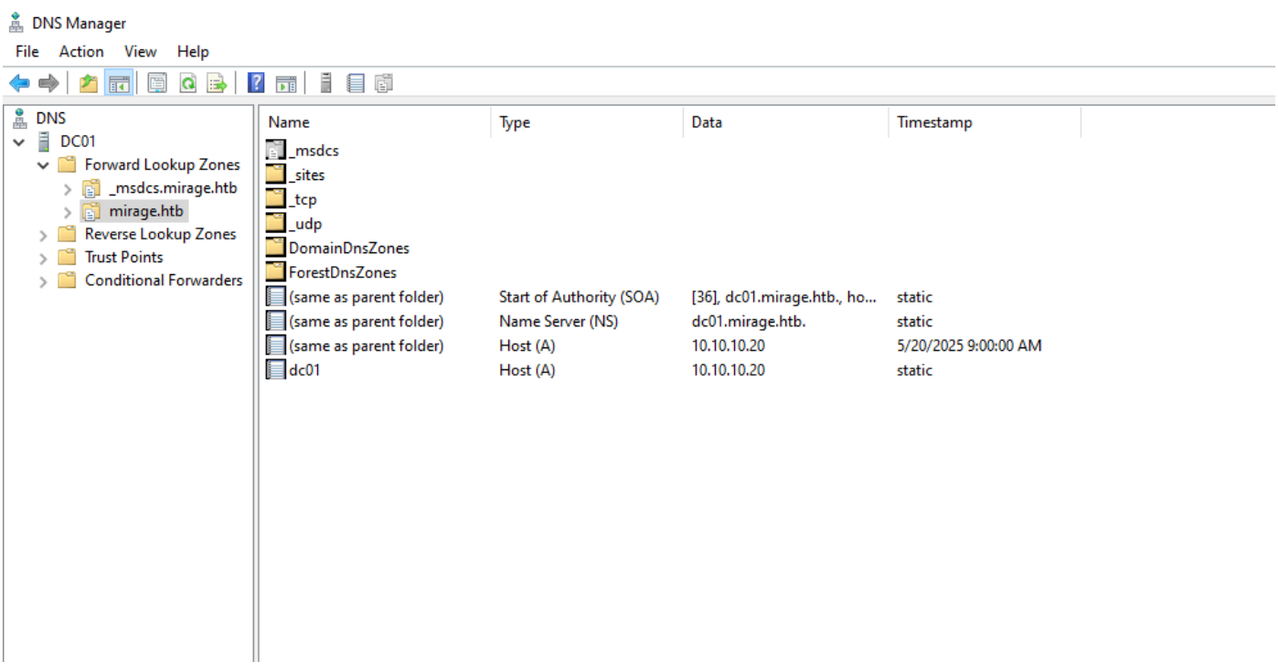
```
PS C:\Users\Dev_Account_A\Desktop\Nats-cli> .\nats -s nats://nats-svc:4222 rtt --user $user --password $password
nats: error: dial tcp: lookup nats-svc: i/o timeout
PS C:\Users\Dev_Account_A\Desktop\Nats-cli>
```

Further investigation confirmed that name resolution failed. DNS could not map the hostname to an IP address.

```
PS C:\Users\Dev_Account_A> nslookup.exe nats-svc
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

*** UnKnown can't find nats-svc: Non-existent domain
PS C:\Users\Dev_Account_A>
```

The Systems Administrator inspected the **dc01.mirage.htb** DNS zone and confirmed that the DNS record for nats-svc was missing.

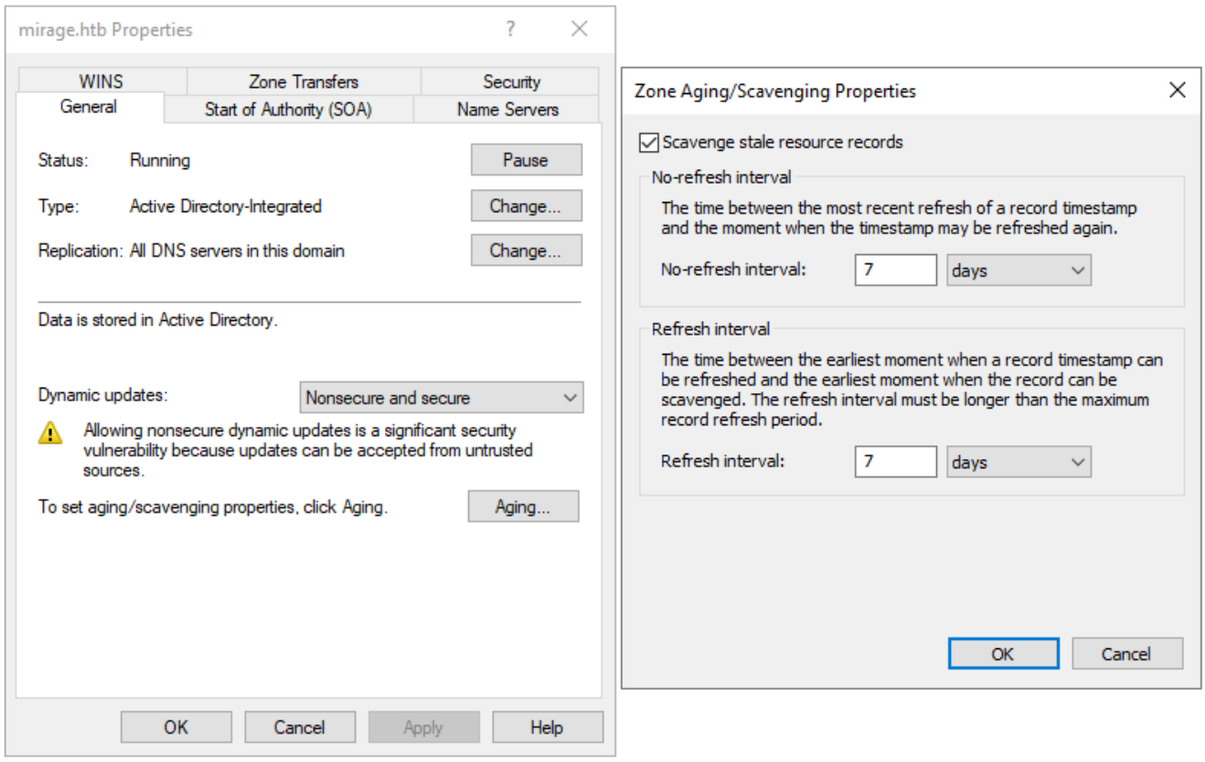


We reviewed the event logs and found Event ID **2501** (scavenging started) and **2502** (scavenging completed), which indicate that DNS scavenging was performed and the nats-svc record was likely deleted automatically.

The DHCP lease records showed the nats-svc machine had been offline for more than 14 days. This aligns with the Development team's rotating shift model (30/15 days), which often results in certain machines being offline for extended periods.

The Mirage DNS server is configured with scavenging enabled, using the default intervals:

- **No-refresh interval**: 7 days
- **Refresh interval**: 7 days



This means any dynamic DNS record that is not refreshed within 14 days is considered stale and can be automatically removed, which is what likely happened to the nats-svc record.

Solution :

To prevent this issue from occurring again, we recommend the following:

1. **Convert nats-svc to a Static Record**
   Static records are not affected by scavenging. Manually converting nats-svc to a static record is the safest solution for services that are not consistently online.
2. **Adjust DNS Scavenging Intervals**
   Extend the scavenging interval to 21–30 days to allow more time before records are considered stale. This is especially useful for systems with infrequent online presence.
3. **Disable Scavenging for the Zone (Optional)**
   Disabling scavenging on the **mirage.htb** zone is possible but not recommended globally, as it affects all dynamic records and could lead to stale record buildup.

Security Consideration :

In development environments, fixed service names such as **nats-svc.mirage.htb** are often hardcoded in applications. If the DNS record is missing, some apps may still attempt to connect to that name. This behavior could be abused by attackers if DNS records are hijacked.

The Security Team should monitor such cases closely to ensure no unauthorized DNS responses are injected or spoofed in the network.