???? NETLOGON/ SYSVOL ??

□□□□□□□□□□□□□□□□□□□□

1. `Get-DfsrGroup` □ `Get-DfsrReplicatedFolder` □□□□□□
   - □ Windows Server 2022/2025 □□□□ cmdlet □□□□□□ PowerShell □□□□□□ RSAT-DFS □□□□□□
   - □□□□ cmdlet □□ `Get-DfsrMember□□□□□□□□ **Invalid□□□** DFS-R □□□□□□□ **S-DNS1 □□□□□□□** □
2. □□ **DFS-R □□**

   ```
   GroupName                    : □□□01
   State                        : Invalid
   ```

   - □□□ DFS-R □□□□□□□□□□□□□□□□□□□□
   - SYSVOL □□□□ S-DNS1 □□□□□□

????

- □□□ DC □□ FSMO □□ **DFS-R □□□□□□□□ SYSVOL**
- DFS-R □□□□ S-DNS1 □□□ → □□□□ DFS-R □□ SYSVOL → □□□□ NETLOGON/ SYSVOL □□
- □□ FSMO □□□□□□□ DC □ SYSVOL □□□□

?????????????

??????? DC ?? SYSVOL ??????

1. □□□□ **S-DNS6 □□□ SYSVOL □□□**

   ```
   dir C:\Windows\SYSVOL\domain
   dir C:\Windows\SYSVOL\sysvol
   ```

   - □□□□ `Policies` □ `Scripts` □□□□
2. □ **S-DNS1 □□□ DFS-R □□**

   ```
   Stop-Service DFSR
   ```

3. □ **S-DNS6 □□ SYSVOL □□□ S-DNS1**

```
robocopy \\S-DNS6\SYSVOL\shuncom.local C:\Windows\SYSVOL\domain /MIR /COPYALL /R:1 /W:1
robocopy \\S-DNS6\SYSVOL\sysvol C:\Windows\SYSVOL\sysvol /MIR /COPYALL /R:1 /W:1
```

4. □□□□□□
   - NTFS □□□
     - SYSTEM → □□□□
     - Domain Admins → □□□□
     - Authenticated Users → □□
5. □□□□

```
net share SYSVOL=C:\Windows\SYSVOL\sysvol /GRANT:"Domain Admins",FULL
net share NETLOGON=C:\Windows\SYSVOL\domain\scripts /GRANT:"Domain Admins",FULL
```

6. □□ **DFS-R** □□

```
Start-Service DFSR
```

7. □□□□□□□

```
net share
\\S-DNS1\SYSVOL
\\S-DNS1\NETLOGON
```

□ □□ □

- □□□ S-DNS1 □□□□□□□ SYSVOL □□
- NETLOGON □ SYSVOL □□□□
- DFS-R □□□□□□□□□□□□□□□□ DC □□□□

□□□□□□□□□□□□ □□□□□ **S-DNS1□ 192.168.0.5□** □□□□□□□□□ **PDC □□□□ PDC Emulator□□□□□□□ GC□** □□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□ □□

? 1. `nltest /dcname:shuncom.local` ??

```
NetGetDCName □□: Status = 2453 0x995 NERR_DCNotFound
```

□□□□□□

- **NetGetDCName API** □□□□□□□□□□□□ □

- □□□□□ **DNS** □□□ **Netlogon** □□□□□□□□□□ □□□□□□□□□□□ SRV □□□□
- □□□□□□□□□ `nltest /dsgetdc` □□□□□□□

? 2. `nltest /dsgetdc:shuncom.local /pdc` ??????

```
DC: \\S-DNS1.shuncom.local
□□: \\192.168.0.5
□□: PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE
FULL_SECRET ...
```

□□□□

- □□ **PDC** □□□□□□ **S-DNS1**□
- □ DC □□□
  - **GC**□□□□□
  - **DS**□□□□□
  - **LDAP**□ **Kerberos**□ **KDC**□ **DNS** □□
  - **WRITABLE**□□□□□
- □□□□□□□□□ `Default-First-Site-Name`
- □□□□□ `PDC`, `KDC`, `DNS_DC` □□□□□ AD □□□□□

> “□ □□ □ S-DNS1 □□□□□□□□□□□□□□□□□□□

? 3. ?????????????

□□□□□□□□□□□□□□□□□□□□□□

```
# □□ SYSVOL □□□□□□
net share | findstr SYSVOL
net share | findstr NETLOGON

# □□ SYSVOL/Netlogon □□
dir \\s-dns1\SYSVOL
dir \\s-dns1\netlogon
```

```
# □□ DFSR □□
dfsrdiag pollad
dfsrdiag backlog /rgname:"Domain System Volume" /rfname:"SYSVOL Share" /smem:s-dns1 /rmem:s-dns1

# □□ AD □□□□
repadmin /replsummary
repadmin /showrepl
repadmin /syncall /AdeP

# □□ DC □□□□
dcdiag /test:advertising /test:sysvol /test:netlogons
```

?? 4. ?? `SYSVOL` ? `NETLOGON` ????

□□□□□□□□□□□□

```
net share SYSVOL=C:\Windows\SYSVOL\sysvol /grant:"Domain Admins",full
net share NETLOGON=C:\Windows\SYSVOL\domain\scripts /grant:"Domain Admins",full
```

? 5. ?????“??? DC”???

□□□□□□□□□□□

```
ipconfig /flushdns
nltest /dsregdns
net stop netlogon
net start netlogon
```

> ❝ □□□□□□□□□□□ SRV □□□

□□□□□□□□□□
□ “□□□□□□□□□□□□□□□□□□□□ +□□□□□□□ ”□
□□□□□□□□□□ S-DNS1 □□□ FSMO □ SYSVOL □□□□□□□□□□

Revision #2
Created 13 October 2025 01:02:58 by Admin
Updated 13 October 2025 02:24:35 by Admin