

???????????????? S-DNS6 ??? SRV ????? S-DNS1 ????? SYSVOL/NETLOGON

???????????????? S-DNS6 ??? SRV ????? S-DNS1
???? SYSVOL/NETLOGON???? DFSR Netlogon DNS ?????
????????????????????????????????????

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

1. ?? S-DNS1 ? S-DNS6 ???

- ? S-DNS1 ??

```
nltest /dsgetdc:shuncom.local /pdc  
repadmin /replsummary  
dfsrdiag /getglobalstate
```

- ? S-DNS6 ??

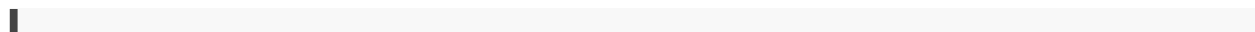
```
net stop netlogon  
dfsrdiag /getglobalstate  
repadmin /replsummary
```

- ?? DFSR ?????????? S-DNS6 ?? Netlogon?????? SRV?

2. ?? DNS ? SYSVOL

- DNS??? shuncom.local ???
 - SYSVOL??? C:\Windows\SYSVOL\sysvol ? C:\Windows\SYSVOL\domain\scripts
??????
-

???? S-DNS6 ?? SRV ??



```
nslookup S-DNS6 s-dns6.shuncom.local _ldap._kerberos._gc SRV
DC
```

1. S-DNS1 DNS

- DNS -> shuncom.local -> _msdcs.shuncom.local
- s-dns6.shuncom.local SRV
 - _ldap._tcp.dc._msdcs.shuncom.local
 - _kerberos._tcp.dc._msdcs.shuncom.local
 - _gc._tcp.shuncom.local
 - _ldap._tcp.gc._msdcs.shuncom.local
- Windows DNS “ ” S-DNS1
- S-DNS6 SRV DNS DC S-DNS6
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\DnsAvoidRegisterRecords

2. S-DNS6 SRV

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" /v
DnsAvoidRegisterRecords /t REG_MULTI_SZ /d "_ldap._tcp._sites._tcp._gc" /f
net stop netlogon
net start netlogon
```

-

3. DNS

- S-DNS1

```
dnscmd /clearcache
ipconfig /flushdns
```

- DNS

```
nltest /dsregdns /server:s-dns1.shuncom.local
```

- SRV

```
nslookup -type=SRV _ldap._tcp.dc._msdcs.shuncom.local
nslookup -type=SRV _kerberos._tcp.dc._msdcs.shuncom.local
nslookup -type=SRV _gc._tcp.shuncom.local
```

???? S-DNS1 ??

SYSVOL/NETLOGON

1. DFSR S-DNS1

```
dfsrdiag /getglobalstate  
dfsrdiag backlog /rgname:"Domain System Volume" /rfname:"SYSVOL Share" /smem:s-dns1  
/rmem:s-dns1
```

- backlog

2. Netlogon

```
net start netlogon  
nltest /dsregdns /server:s-dns1.shuncom.local
```

- SYSVOL/NETLOGON

```
net share  
dir \\s-dns1\SYSVOL  
dir \\s-dns1\NETLOGON
```

-

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

3. DFSR AD S-DNS1 → S-DNS6

```
repadmin /syncall /AdeP  
repadmin /showrepl
```

??????

1. AD

```
dcldiag /test:advertising /test:netlogons /test:sysvol
```

- S-DNS1
- S-DNS6 SRV

2. SRV

```
nslookup -type=SRV _ldap._tcp.dc._msdcs.shuncom.local
nslookup -type=SRV _kerberos._tcp.dc._msdcs.shuncom.local
nslookup -type=SRV _gc._tcp.shuncom.local
```

- S-DNS1 [] DC []
- S-DNS6 []

3. [] **SYSVOL/NETLOGON** [] []

- [] DC []

```
\\s-dns1\SYSVOL
\\s-dns1\netlogon
```

[] []

- S-DNS6 [] Netlogon [] AD [] SRV []
- [] Netlogon []
- [] DNS []
- [] S-DNS1 [] AD [] DNS []

```
repadmin /syncall /AdeP
nltest /dsregdns /server:s-dns1.shuncom.local
ipconfig /registerdns
```

[]

- **DFSRDIAG** [] **S-DNS1** [] **S-DNS6** [] 1355 / 1717 []
- [] **Netlogon** [] []
- **Netlogon** [] [] SYSVOL/NETLOGON [] ipconfig /registerdns []

[] DFSR [] DNS [] Netlogon [] S-DNS1 [] “ [] ”
PDC/SYSVOL/NETLOGON []

? ???? ?

1. **S-DNS6** [] **Netlogon** → [] AD [] DNS [] SRV []
2. **S-DNS1** **DFSR** [] → ReplicationState [] Backlog []
3. **DNS SRV** [] → DsGetDcName [] S-DNS6 [] DFSR/Netlogon []
4. **Netlogon** [] → [] S-DNS1 [] DNS [] AD [] S-DNS6 []
SYSVOL/NETLOGON [] DFSR []

? ?????????????? + ??????

?? 1????? S-DNS6 Netlogon

```
# S-DNS6 操作
net stop netlogon
sc config netlogon start= disabled
```

- 操作 SRV 操作

?? 2???? DNS ? S-DNS6 SRV

- 操作 DNS 操作 → 操作 → `_msdcs.shuncom.local`
- 操作 S-DNS6 操作 SRV 操作
 - `_ldap._tcp.dc._msdcs.shuncom.local`
 - `_kerberos._tcp.dc._msdcs.shuncom.local`
 - `_gc._tcp.shuncom.local`
- 操作 PowerShell 操作

```
Import-Module DNSServer
Remove-DnsServerResourceRecord -ZoneName "_msdcs.shuncom.local" -Name
"_ldap._tcp.dc._msdcs.shuncom.local" -RRType "SRV" -ComputerName S-DNS1
```

?? 3??? S-DNS1 ????? Netlogon / SYSVOL

```
# 操作 Netlogon
net stop netlogon
net start netlogon

# 操作 DC SRV
nltest /dsregdns /server:S-DNS1.shuncom.local
```

- 操作 SYSVOL / NETLOGON 操作

```
net share
dir \\S-DNS1\SYSVOL
dir \\S-DNS1\netlogon
```