

```
dcdiag /v /c /e /f:"%userprofile%\Desktop\dcdiag.txt"
```

## Directory Server Diagnosis

### Performing initial setup:

Trying to find home server...

\* Verifying that the local machine Win2016DC2, is a Directory Server.

Home Server = Win2016DC2

\* Connecting to directory service on server Win2016DC2.

\* Identified AD Forest.

Collecting AD specific global data

\* Collecting site info.

Calling

```
ldap_search_init_page(hld,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyP  
roductions,DC=com,LDAP_SCOPE_SUBTREE,(objectCategory=ntDSSiteSettings),.....
```

The previous call succeeded

Iterating through the sites

Looking at base site object: CN=NTDS Site

```
Settings,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyP  
roductions,DC=com
```

Getting ISTG and options for the site

Looking at base site object: CN=NTDS Site

```
Settings,CN=Mikrotek,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyPro  
ductions,DC=com
```

Getting ISTG and options for the site

\* Identifying all servers.

Calling

```
ldap_search_init_page(hld,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyP  
roductions,DC=com,LDAP_SCOPE_SUBTREE,(objectClass=ntDSDsa),.....
```

The previous call succeeded....

The previous call succeeded

Iterating through the list of servers

Getting information for the server CN=NTDS

```
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com
```

objectGuid obtained

InvocationID obtained

dnsHostname obtained  
site info obtained  
All the info for the server collected  
\* Identifying all NC cross-refs.

\* Found 1 DC(s). Testing 1 of them.

Done gathering initial info.

Doing initial required tests

Testing server: HQ-Homelab\WIN2016DC2

Starting test: Connectivity

\* Active Directory LDAP Services Check  
Determining IP4 connectivity  
\* Active Directory RPC Services Check  
..... WIN2016DC2 passed test Connectivity

Doing primary tests

Testing server: HQ-Homelab\WIN2016DC2

Starting test: Advertising

The DC WIN2016DC2 is advertising itself as a DC and having a DS.  
The DC WIN2016DC2 is advertising as an LDAP server  
The DC WIN2016DC2 is advertising as having a writeable directory  
The DC WIN2016DC2 is advertising as a Key Distribution Center  
The DC WIN2016DC2 is advertising as a time server  
The DS WIN2016DC2 is advertising as a GC.  
..... WIN2016DC2 passed test Advertising

Starting test: CheckSecurityError

\* Dr Auth: Beginning security errors check!  
Found KDC WIN2016DC2 for domain HomeLab.TechSavvyProductions.com in  
site HQ-Homelab

Checking machine account for DC WIN2016DC2 on DC WIN2016DC2.  
\* SPN found  
:LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com  
\* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com  
\* SPN found :LDAP/WIN2016DC2  
\* SPN found  
:LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB  
\* SPN found  
:LDAP/60228dba-cbc8-4304-868a-28f53a302f46.\_msdcs.HomeLab.TechSavvyProductions.com  
\* SPN found  
:E3514235-4B06-11D1-AB04-00C04FC2DCD2/60228dba-cbc8-4304-868a-28f53a302f46/HomeLab.TechSavvyProductions.com  
\* SPN found  
:HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com  
\* SPN found :HOST/Win2016DC2.HomeLab.TechSavvyProductions.com  
\* SPN found :HOST/WIN2016DC2  
\* SPN found  
:HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB  
\* SPN found  
:GC/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com  
[WIN2016DC2] DsReplicaGetInfo(KCC\_DS\_CONNECT\_FAILURES) failed with error 8453,

Replication access was denied..

[WIN2016DC2] Unable to query the list of KCC connection failures.

Continuing...

[WIN2016DC2] No security related replication errors were found on this DC! To target the connection to a

specific source DC use /ReplSource:<DC>.

..... WIN2016DC2 passed test CheckSecurityError

Starting test: CutoffServers

\* Configuration Topology Aliveness Check  
\* Analyzing the alive system replication topology for  
DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com.  
\* Performing upstream (of target) analysis.

- \* Performing downstream (of target) analysis.
- \* Analyzing the alive system replication topology for DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.
- \* Analyzing the alive system replication topology for CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.
- \* Analyzing the alive system replication topology for CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.
- \* Analyzing the alive system replication topology for DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.

..... WIN2016DC2 passed test CutoffServers

Starting test: FrsEvent

- \* The File Replication Service Event log test

Skip the test because the server is running DFSR.

..... WIN2016DC2 passed test FrsEvent

Starting test: DFSREvent

The DFS Replication Event Log.

There are warning or error events within the last 24 hours after the SYSVOL has been shared. Failing SYSVOL

replication problems may cause Group Policy problems.

An error event occurred. EventID: 0xC0001390

Time Generated: 06/17/2025 04:15:47

Event String:

The DFS Replication service failed to communicate with partner WIN2016DC3 for replication group Domain System Volume. This error can occur if the host is unreachable, or if the DFS Replication service is not running on the server.

Partner DNS Address: Win2016dc3.HomeLab.TechSavvyProductions.com

Optional data if available:

Partner WINS Address: Win2016dc3

Partner IP Address: 192.168.0.232

The service will retry the connection periodically.

Additional Information:

Error: 1722 (The RPC server is unavailable.)

Connection ID: 80173626-A8CB-495C-9654-730B01A95E34

Replication Group ID: 7E84258A-AF73-4C40-AFAC-AB7C33CB14E7

An error event occurred. EventID: 0xC0001390

Time Generated: 06/17/2025 12:20:37

Event String:

The DFS Replication service failed to communicate with partner WIN2016DC3 for replication group Domain System Volume. This error can occur if the host is unreachable, or if the DFS Replication service is not running on the server.

Partner DNS Address: Win2016dc3.HomeLab.TechSavvyProductions.com

Optional data if available:

Partner WINS Address: Win2016dc3

Partner IP Address: 192.168.0.232

The service will retry the connection periodically.

Additional Information:

Error: 1722 (The RPC server is unavailable.)

Connection ID: 80173626-A8CB-495C-9654-730B01A95E34

Replication Group ID: 7E84258A-AF73-4C40-AFAC-AB7C33CB14E7

An error event occurred. EventID: 0xC0001390

Time Generated: 06/17/2025 20:25:11

Event String:

The DFS Replication service failed to communicate with partner WIN2016DC3 for replication group Domain System Volume. This error can occur if the host is unreachable, or if the DFS Replication service is not running on the server.

Partner DNS Address: Win2016dc3.HomeLab.TechSavvyProductions.com

Optional data if available:

Partner WINS Address: Win2016dc3

Partner IP Address: 192.168.0.232

The service will retry the connection periodically.

Additional Information:

Error: 1722 (The RPC server is unavailable.)

Connection ID: 80173626-A8CB-495C-9654-730B01A95E34

Replication Group ID: 7E84258A-AF73-4C40-AFAC-AB7C33CB14E7

An error event occurred. EventID: 0xC00004B2

Time Generated: 06/18/2025 00:06:32

Event String:

The DFS Replication service failed to contact domain controller to access configuration information. Replication is stopped. The service will try again during the next configuration polling cycle, which will occur in 60 minutes. This event can be caused by TCP/IP connectivity, firewall, Active Directory Domain Services, or DNS issues.

Additional Information:

Error: 160 (One or more arguments are not correct.)

..... WIN2016DC2 failed test DFSREvent

Starting test: SysVolCheck

\* The File Replication Service SYSVOL ready test  
File Replication Service's SYSVOL is ready  
..... WIN2016DC2 passed test SysVolCheck

Starting test: FrsSysVol

\* The File Replication Service SYSVOL ready test  
File Replication Service's SYSVOL is ready  
..... WIN2016DC2 passed test FrsSysVol

Starting test: KccEvent

\* The KCC Event log test

Found no KCC errors in "Directory Service" Event log in the last 15 minutes.  
..... WIN2016DC2 passed test KccEvent

Starting test: KnowsOfRoleHolders

Role Schema Owner = CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com  
Role Domain Owner = CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com  
Role PDC Owner = CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com  
Role Rid Owner = CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com  
Role Infrastructure Update Owner = CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com  
..... WIN2016DC2 passed test KnowsOfRoleHolders

Starting test: MachineAccount

Checking machine account for DC WIN2016DC2 on DC WIN2016DC2.  
\* SPN found  
:LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com  
\* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com  
\* SPN found :LDAP/WIN2016DC2  
\* SPN found  
:LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB  
\* SPN found  
:LDAP/60228dba-cbc8-4304-868a-28f53a302f46.\_msdcs.HomeLab.TechSavvyProductions.com  
\* SPN found  
:E3514235-4B06-11D1-AB04-00C04FC2DCD2/60228dba-cbc8-4304-868a-28f53a302f46/HomeLab.TechSavvyProductions.com  
\* SPN found  
:HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com  
\* SPN found :HOST/Win2016DC2.HomeLab.TechSavvyProductions.com  
\* SPN found :HOST/WIN2016DC2

\* SPN found  
:HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB  
\* SPN found  
:GC/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com

..... WIN2016DC2 passed test MachineAccount

Starting test: NCSecDesc

\* Security Permissions check for all NC's on DC WIN2016DC2.

\* Security Permissions Check for

DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(NDNC,Version 3)

\* Security Permissions Check for

DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(NDNC,Version 3)

\* Security Permissions Check for

CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(Schema,Version 3)

\* Security Permissions Check for

CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(Configuration,Version 3)

\* Security Permissions Check for

DC=HomeLab,DC=TechSavvyProductions,DC=com  
(Domain,Version 3)

..... WIN2016DC2 passed test NCSecDesc

Starting test: NetLogons

\* Network Logons Privileges Check

Verified share \\WIN2016DC2\netlogon

Verified share \\WIN2016DC2\sysvol

[WIN2016DC2] User credentials does not have permission to perform this operation.

The account used for this test must have network logon privileges

for this machine's domain.

..... WIN2016DC2 failed test NetLogons

Starting test: ObjectsReplicated

WIN2016DC2 is in domain DC=HomeLab,DC=TechSavvyProductions,DC=com  
Checking for CN=WIN2016DC2,OU=Domain  
Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com in domain  
DC=HomeLab,DC=TechSavvyProductions,DC=com on 1 servers  
Object is up-to-date on all servers.  
Checking for CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com in domain  
CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com on 1 servers  
Object is up-to-date on all servers.  
..... WIN2016DC2 passed test ObjectsReplicated

Starting test: OutboundSecureChannels

\* The Outbound Secure Channels test  
\*\* Did not run Outbound Secure Channels test because /testdomain: was not  
entered

..... WIN2016DC2 passed test OutboundSecureChannels

Starting test: Replications

\* Replications Check  
[Replications Check,WIN2016DC2] DsReplicaGetInfo(PENDING\_OPS, NULL)  
failed, error 0x2105

"Replication access was denied."

..... WIN2016DC2 failed test Replications

Starting test: RidManager

\* Available RID Pool for the Domain is 14600 to 1073741823  
\* Win2016DC2.HomeLab.TechSavvyProductions.com is the RID Master  
\* DsBind with RID Master was successful  
\* rIDAllocationPool is 4100 to 4599  
\* rIDPreviousAllocationPool is 4100 to 4599  
\* rIDNextRID: 4101  
..... WIN2016DC2 passed test RidManager

Starting test: Services

- \* Checking Service: EventSystem
  - \* Checking Service: RpcSs
  - \* Checking Service: NTDS  
Could not open NTDS Service on WIN2016DC2, error 0x5 "Access is denied."
  
  - \* Checking Service: DnsCache
  - \* Checking Service: DFSR
  - \* Checking Service: lsmServ
  - \* Checking Service: kdc
  - \* Checking Service: SamSs
  - \* Checking Service: LanmanServer
  - \* Checking Service: LanmanWorkstation
  - \* Checking Service: w32time
  - \* Checking Service: NETLOGON
- ..... WIN2016DC2 failed test Services

Starting test: SystemLog

- \* The System Event log test  
An error event occurred. EventID: 0x0000272C

Time Generated: 06/17/2025 23:43:49

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 1678 (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/17/2025 23:43:49

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 1678 (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/17/2025 23:43:49

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 1678 (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/17/2025 23:43:49

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 1678 (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x00002720

Time Generated: 06/17/2025 23:47:37

Event String:

The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID

{D63B10C5-BB46-4990-A94F-E40B9D520160}

and APPID

{9CA88EE3-ACB7-47C8-AFC4-AB702511C276}

to the user HOMELAB\HomeBoss SID (S-1-5-21-3892272843-2021369796-1445886767-1103) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.

An error event occurred. EventID: 0x0000272C

Time Generated: 06/17/2025 23:53:49

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 1678 (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/17/2025 23:53:49

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 1678 (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/17/2025 23:53:49

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 1678 (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/17/2025 23:53:49

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 1678 (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/18/2025 00:03:49

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 1678 (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/18/2025 00:03:49

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 1678 (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/18/2025 00:03:49

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 1678 (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/18/2025 00:03:49

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 1678 (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x00000029

Time Generated: 06/18/2025 00:06:09

Event String: Hypervisor launch failed; Either VMX not present or not enabled in BIOS.

A warning event occurred. EventID: 0x000000DB

Time Generated: 06/18/2025 00:06:10

Event String: The driver \Driver\vmbsr failed to load for the device ROOT\VMBus\0000.

A warning event occurred. EventID: 0x80040020

Time Generated: 06/18/2025 00:06:10

Event String:

The driver detected that the device \Device\Harddisk1\DR1 has its write cache enabled. Data corruption may occur.

A warning event occurred. EventID: 0x80040020

Time Generated: 06/18/2025 00:06:10

Event String:

The driver detected that the device \Device\Harddisk1\DR1 has its write cache enabled. Data corruption may occur.

A warning event occurred. EventID: 0x80040020

Time Generated: 06/18/2025 00:06:10

Event String:

The driver detected that the device \Device\Harddisk1\DR1 has its write cache enabled. Data corruption may occur.

A warning event occurred. EventID: 0x000003F6

Time Generated: 06/18/2025 00:06:13

Event String:

Name resolution for the name  
\_ldap.\_tcp.dc.\_msdcs.HomeLab.TechSavvyProductions.com. timed out after none of  
the configured DNS servers responded.

An error event occurred. EventID: 0x00000469

Time Generated: 06/18/2025 00:06:33

Event String:

The processing of Group Policy failed because of lack of network connectivity to a domain controller. This may be a transient condition. A success message would be generated once the machine gets connected to the domain controller and Group Policy has successfully processed. If you do not see a success message for several hours, then contact your administrator.

An error event occurred. EventID: 0x00000469

Time Generated: 06/18/2025 00:06:35

Event String:

The processing of Group Policy failed because of lack of network connectivity to a domain controller. This may be a transient condition. A success message would be generated once the machine gets connected to the domain controller and Group Policy has successfully processed. If you do not see a success message for several hours, then contact your administrator.

An error event occurred. EventID: 0x0000168E

Time Generated: 06/18/2025 00:07:22

Event String:

The dynamic registration of the DNS record '\_ldap.\_tcp.HomeLab.TechSavvyProductions.com. 600 IN SRV 0 100 389 win2016dc2.homelab.techsavvyproductions.com.' failed on the following DNS server:

DNS server IP address: 2603:5:21d0::a

Returned Response Code (RCODE): 1

Returned Status Code: 9001

For computers and users to locate this domain controller, this record must be registered in DNS.

USER ACTION

Determine what might have caused this failure, resolve the problem, and initiate registration of the DNS records by the domain controller. To determine what might have caused this failure, run DCdiag.exe. To learn more about DCdiag.exe, see Help and Support Center. To initiate registration of the DNS records by this domain controller, run 'nltest.exe /dsregdns' from the command prompt on the domain controller or restart Net Logon service.

Or, you can manually add this record to DNS, but it is not recommended.

#### ADDITIONAL DATA

Error Value: DNS server unable to interpret format.

A warning event occurred. EventID: 0x000003F6

Time Generated: 06/18/2025 00:07:22

Event String:

Name resolution for the name TechSavvyProductions.com timed out after none of the configured DNS servers responded.

An error event occurred. EventID: 0x00002720

Time Generated: 06/18/2025 00:07:24

Event String:

The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID

{8D8F4F83-3594-4F07-8369-FC3C3CAE4919}

and APPID

{F72671A9-012C-4725-9D2F-2A4D32D65169}

to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.

An error event occurred. EventID: 0x00072790

Time Generated: 06/18/2025 00:07:27

Event String:

The WinRM service is not listening for HTTP requests because there was a failure binding to the URL (http://+:80/wsman/) in HTTP.SYS.

No remote requests will be serviced on that URL.

User Action

Please use "netsh http" to check if ACL for URL (http://+:80/wsman/) is set to Network Service.

Additional Data

The error code received from HTTP.sys is 5: %%5

A warning event occurred. EventID: 0x000727AA

Time Generated: 06/18/2025 00:07:27

Event String:

The WinRM service failed to create the following SPNs:  
WSMAN/Win2016DC2.HomeLab.TechSavvyProductions.com; WSMAN/Win2016DC2.

Additional Data

The error received was 8344: %%8344.

User Action

The SPNs can be created by an administrator using setspn.exe utility.

An error event occurred. EventID: 0x0000272C

Time Generated: 06/18/2025 00:07:28

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 120c (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/18/2025 00:07:28

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 120c (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/18/2025 00:07:28

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 120c (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/18/2025 00:07:28

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 120c (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x00002720

Time Generated: 06/18/2025 00:28:31

Event String:

The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID

{D63B10C5-BB46-4990-A94F-E40B9D520160}

and APPID

{9CA88EE3-ACB7-47C8-AFC4-AB702511C276}

to the user HOMELAB\HomeBoss SID (S-1-5-21-3892272843-2021369796-1445886767-1103) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.

An error event occurred. EventID: 0x00002720

Time Generated: 06/18/2025 00:28:49

Event String:

The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID

{D63B10C5-BB46-4990-A94F-E40B9D520160}

and APPID

{9CA88EE3-ACB7-47C8-AFC4-AB702511C276}

to the user HOMELAB\HomeBoss SID (S-1-5-21-3892272843-2021369796-1445886767-1103) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.

..... WIN2016DC2 failed test SystemLog

Starting test: Topology

\* Configuration Topology Integrity Check

- \* Analyzing the connection topology for  
DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.
- \* Analyzing the connection topology for  
DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.
- \* Analyzing the connection topology for  
CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.
- \* Analyzing the connection topology for  
CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.
- \* Analyzing the connection topology for  
DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.

..... WIN2016DC2 passed test Topology

Starting test: VerifyEnterpriseReferences

..... WIN2016DC2 passed test VerifyEnterpriseReferences

Starting test: VerifyReferences

The system object reference (serverReference)

CN=WIN2016DC2,OU=Domain  
Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com and backlink on

CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com are

correct.

The system object reference (serverReferenceBL)

CN=WIN2016DC2,CN=Topology,CN=Domain System  
Volume,CN=DFSR-GlobalSettings,CN=System,DC=HomeLab,DC=TechSavvyProductions,DC=com

and backlink on

CN=NTDS

Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com

are correct.

The system object reference (msDFSR-ComputerReferenceBL)

CN=WIN2016DC2,CN=Topology,CN=Domain System

Volume,CN=DFSR-GlobalSettings,CN=System,DC=HomeLab,DC=TechSavvyProductions,DC=com

and backlink on CN=WIN2016DC2,OU=Domain

Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com are correct.

..... WIN2016DC2 passed test VerifyReferences

Starting test: VerifyReplicas

..... WIN2016DC2 passed test VerifyReplicas

Starting test: DNS

DNS Tests are running and not hung. Please wait a few minutes...

See DNS test in enterprise tests section for results

..... WIN2016DC2 failed test DNS

Running partition tests on : ForestDnsZones

Starting test: CheckSDRefDom

..... ForestDnsZones passed test CheckSDRefDom

Starting test: CrossRefValidation

..... ForestDnsZones passed test CrossRefValidation

Running partition tests on : DomainDnsZones

Starting test: CheckSDRefDom

..... DomainDnsZones passed test CheckSDRefDom

Starting test: CrossRefValidation

..... DomainDnsZones passed test CrossRefValidation

Running partition tests on : Schema

Starting test: CheckSDRefDom

..... Schema passed test CheckSDRefDom

Starting test: CrossRefValidation

..... Schema passed test CrossRefValidation

Running partition tests on : Configuration

Starting test: CheckSDRefDom

..... Configuration passed test CheckSDRefDom

Starting test: CrossRefValidation

..... Configuration passed test CrossRefValidation

Running partition tests on : HomeLab

Starting test: CheckSDRefDom

..... HomeLab passed test CheckSDRefDom

Starting test: CrossRefValidation

..... HomeLab passed test CrossRefValidation

Running enterprise tests on : HomeLab.TechSavvyProductions.com

Starting test: DNS

Test results for domain controllers:

DC: Win2016DC2.HomeLab.TechSavvyProductions.com

Domain: HomeLab.TechSavvyProductions.com

TEST: Authentication (Auth)

Authentication test: Successfully completed

TEST: Basic (Basc)

The OS Microsoft Windows Server 2016 Standard (Service Pack level: 0.0) is supported.

NETLOGON service is running

kdc service is running

DNSCACHE service is running

DNS service is running

DC is a DNS server

Network adapters information:

Adapter [00000002] Microsoft Hyper-V Network Adapter:

MAC address is 00:15:5D:0A:02:01

IP Address is static

IP address: 192.168.0.231, fe80::bc12:2097:a01a:a853

DNS servers:

192.168.0.231 (WIN2016DC2) [Valid]

127.0.0.1 (WIN2016DC2) [Valid]

Warning:

192.168.0.1 (<name unavailable>) [Invalid]

Warning: adapter [00000002] Microsoft Hyper-V Network Adapter has invalid DNS server:

192.168.0.1 (<name unavailable>)

The A host record(s) for this DC was found

The SOA record for the Active Directory zone was found

Warning: no DNS RPC connectivity (error or non Microsoft DNS server is running)

[Error details: 5 (Type: Win32 - Description: Access is denied.)]

Summary of test results for DNS servers used by the above domain controllers:

DNS server: 192.168.0.1 (<name unavailable>)

1 test failure on this DNS server

Name resolution is not functional.

\_ldap.\_tcp.HomeLab.TechSavvyProductions.com. failed on the DNS server 192.168.0.1

[Error details: 9003 (Type: Win32 - Description: DNS name does not exist.)]

DNS server: 192.168.0.231 (WIN2016DC2)

All tests passed on this DNS server

Name resolution is functional.\_ldap.\_tcp SRV record for the forest root domain is registered

Summary of DNS test results:

Auth Basc Forw Del Dyn RReg Ext

---

Domain: HomeLab.TechSavvyProductions.com

Win2016DC2                    PASS WARN n/a n/a n/a n/a n/a

..... HomeLab.TechSavvyProductions.com passed test DNS

Starting test: LocatorCheck

GC Name: \\Win2016DC2.HomeLab.TechSavvyProductions.com

Locator Flags: 0xe003f3fd

PDC Name: \\Win2016DC2.HomeLab.TechSavvyProductions.com

Locator Flags: 0xe003f3fd

Time Server Name: \\Win2016DC2.HomeLab.TechSavvyProductions.com

Locator Flags: 0xe003f3fd

Preferred Time Server Name:

\\Win2016DC2.HomeLab.TechSavvyProductions.com

Locator Flags: 0xe003f3fd

KDC Name: \\Win2016DC2.HomeLab.TechSavvyProductions.com

Locator Flags: 0xe003f3fd

..... HomeLab.TechSavvyProductions.com passed test LocatorCheck

Starting test: FsmoCheck

GC Name: \\Win2016DC2.HomeLab.TechSavvyProductions.com

Locator Flags: 0xe003f3fd

PDC Name: \\Win2016DC2.HomeLab.TechSavvyProductions.com

Locator Flags: 0xe003f3fd

Time Server Name: \\Win2016DC2.HomeLab.TechSavvyProductions.com

Locator Flags: 0xe003f3fd

Preferred Time Server Name:

\\Win2016DC2.HomeLab.TechSavvyProductions.com

Locator Flags: 0xe003f3fd

KDC Name: \\Win2016DC2.HomeLab.TechSavvyProductions.com

Locator Flags: 0xe003f3fd

..... HomeLab.TechSavvyProductions.com passed test FsmoCheck

Starting test: Intersite

Doing intersite inbound replication test on site HQ-Homelab:

Locating & Contacting Intersite Topology Generator (ISTG) ...

The ISTG for site HQ-Homelab is: WIN2016DC2.

\*\*\*Error: On server WIN2016DC2, DsReplicaGetInfo() failed, error: 0x2105

"Replication access was denied."

Inbound intersite replication test cannot proceed.

Skipping site Mikrotek, this site is outside the scope provided by the command line arguments provided.

..... HomeLab.TechSavvyProductions.com failed test Intersite

You're seeing a **common post-cleanup issue** after manually removing a failed DC: the surviving DC (WIN2016DC2) is showing **permission-related DCdiag failures** for services, replication, and network logon privileges. These failures are often due to:

- Incomplete cleanup of the demoted/removed DC.
- Lack of **elevated permissions** for the account running DCdiag.
- Damaged **DC-level ACLs, missing group memberships, or SYSVOL inconsistencies.**

Below is a **step-by-step diagnostic and fix guide for each error** you posted:

---

### **Test:** Services

#### **Error:**

Could not open NTDS Service on WIN2016DC2, error 0x5 "Access is denied."

#### **Fix:**

This is likely because you're running `dcdiag` without elevated privileges or from a **non-Domain Admin** account.

#### **Steps:**

1. **Log in as a Domain Admin** (or equivalent admin account).
2. Open **Command Prompt or PowerShell as Administrator**.
3. Rerun `dcdiag`:

```
dcdiag /v /c /e /f:"%userprofile%\Desktop\dcdiag.txt"
```

If the error persists:

4. Verify your user is a member of:

```
whoami  
net user %username% /domain
```

Ensure you're in:

- Domain Admins
- Enterprise Admins

```
C:\Users\HomeBoss>whoami
homelab\homeboss

C:\Users\HomeBoss>net user %username% /domain
User name           HomeBoss
Full Name           HomeBoss
Comment
User's comment
Country/region code 000 (System Default)
Account active       Yes
Account expires      Never

Password last set    2/12/2024 9:18:38 AM
Password expires     Never
Password changeable  2/13/2024 9:18:38 AM
Password required    Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon           6/19/2025 3:53:00 AM

Logon hours allowed  All

Local Group Memberships  *DnsAdmins           *Remote Desktop Users
Global Group memberships *Linux Admins        *Domain Users
                        *Schema Admins       *Domain Admins
                        *Enterprise Admins

The command completed successfully.
```

---

## **Test:** Replications

### **Error:**

DsReplicaGetInfo(PENDING\_OPS, NULL) failed, error 0x2105 — Replication access was denied.

### **Fix:**

This error means that the current user does **not have permission to query** AD replication metadata.

### **Steps:**

1. Ensure you're running as a member of Domain Admins.
2. Ensure the **NTDS Settings object** ACL is intact:

### Using ADSIEdit:

- adsiedit.msc
  - **Connect to: Configuration**
  - **Go to:**
  - CN=Sites > CN=HQ-Homelab > CN=Servers > CN=WIN2016DC2 > CN=NTDS Settings
  - **Right-click** CN=NTDS Settings → **Properties** → **Security**
  - Ensure your user (or Domain Admins group) has **Read/Write/Replicate Directory Changes** permissions.
3. Force reset ACLs (use with caution):

```
dscls "CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=homelab,DC=techsavvyproductions,DC=com" /I:T /G "Domain Admins:GA"
```

```
C:\Users\HomeBoss>dscls "CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=homelab,DC=techsavvyproductions,DC=com" /I:T /G "Domain Admins:GA"

Specified operation failed with ldap error:
    00000005: SecErr: DSID-03152DB2, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0

    Insufficient Rights
.
Access is denied.

The command failed to complete successfully.
```

4. Restart NTDS:

```
net stop ntds
net start ntds
```

---

### **Test:** NetLogons

#### **Error:**

User credentials does not have permission to perform this operation.

#### **Fix:**

This is a **missing or broken trust between DC and domain**, usually tied to:

- Broken Netlogon service
- Computer account trust problems
- SYSVOL/NETLOGON share permission issues

## Steps:

1. Ensure **Netlogon** and **NTFRS** or **DFS-R** services are running:

```
Get-Service Netlogon, NTFRS, DFSR
```

Start them if stopped:

```
Start-Service Netlogon
```

2. Verify `\\WIN2016DC2\NETLOGON` and `\\WIN2016DC2\SYSVOL` are shared and accessible:
  - o From another machine:
  - o `net use \\WIN2016DC2\netlogon`
3. Confirm machine trust account is not broken:

```
nltest /sc_verify:homelab.techsavvyproductions.com
```

If trust is broken:

```
netdom resetpwd /server:WIN2016DC2 /userd:administrator /passwordd:*
```

Then restart `Netlogon`.

---

## Test: Intersite

**Error:**

DsReplicaGetInfo() failed, error: 0x2105 — Replication access was denied.

## Fix:

Same root cause as the **Replications** test — permissions missing or corrupted ACLs.

## Steps:

1. Double-check the **ISTG** role is held by `WIN2016DC2`:

```
Get-ADObject -Filter {objectClass -eq "nTDSDSA"} -SearchBase "CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=ho  
melab,DC=techsavvyproductions,DC=com" -Properties * | Select-Object  
interSiteTopologyGenerator
```

2. If ISTG is not working:
  - o Re-register it:
  - o `repadmin /rehost <SiteName>`

3. Clean stale connections manually from `dssite.msc` or use:

```
repadmin /removelingerobjects WIN2016DC2  
"dc=homelab,dc=techsavvyproductions,dc=com" /advisory_mode
```

If safe:

```
repadmin /removelingerobjects WIN2016DC2  
"dc=homelab,dc=techsavvyproductions,dc=com"
```

---

## Post-Fix Verification

After applying all fixes, rerun:

```
dcdiag /v /c /e /f:"%userprofile%\Desktop\dcdiag-clean.txt"
```

Also run:

```
repadmin /replsummary  
repadmin /showrepl
```

Check:

- No replication failures
- SYSVOL is accessible
- DNS is resolving correctly

```
C:\Users\HomeBoss>repadmin /showrepl  
  
Repadmin: running command /showrepl against full DC localhost  
HQ-Homelab\WIN2016DC2  
DSA Options: IS_GC  
Site Options: (none)  
DSA object GUID: 60228dba-cbc8-4304-868a-28f53a302f46  
DSA invocationID: 7a35f1f8-1dce-4399-9264-25fdb678ef21
```

---

## Optional Tools

Tool	Purpose
<b>Repadmin</b>	Check replication health, force replication
<b>ADSIEdit</b>	Manually inspect/repair AD objects and ACLs
<b>Dsacls</b>	View and modify AD permissions

<b>Tool</b>	<b>Purpose</b>
<b>Netdom</b>	Repair trust and reset passwords
<b>Dcdiag</b>	Full AD health diagnostics

---

Would you like a **scripted checklist** or **PowerShell toolset** to run all these post-recovery checks automatically?

Based on your full `dcdiag` output, your recovered domain controller `WIN2016DC2` is functional but has **several critical errors** mostly caused by:

- **Insufficient access rights** (DC permissions or DCOM)
  - **SYSVOL/DFSR replication issues**
  - **Service misconfigurations**
  - **Network name resolution and DNS registration failures**
- 

## **STEP-BY-STEP TROUBLESHOOTING GUIDE FOR ALL ERRORS**

---

### **1. Replication access was denied (Error 0x2105, Test: Replications & CheckSecurityError)**

**Root Cause:** The current user or DC computer account lacks permission to query replication metadata — often caused by ACL corruption after manual DC removal.

#### **Fix:**

##### **1. Ensure your admin account is in these groups:**

- o Domain Admins
- o Enterprise Admins
- o Administrators

##### **2. Take ownership of the NTDS Settings object:**

- o Open `adsiedit.msc`
- o Connect to the **Configuration context**
- o Navigate to:

```
ini
CopyEdit
CN=NTDS
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configu
ration,...
```

- o Right-click → **Properties** → Security → Advanced
  - o Change **Owner** to your account or Domain Admins
  - o Then assign **Full Control**
3. **Restart NTDS:**

```
powershell
CopyEdit
net stop ntfs
net start ntfs
```

4. **Verify replication:**

```
powershell
CopyEdit
repadmin /replsummary
repadmin /showrepl
```

---

## 2. Test services – Access Denied on NTDS

**Root Cause:** dcdiag run with insufficient privileges or permission corruption on NTDS service.

### **Fix:**

1. **Run PowerShell or CMD as Administrator**
2. Confirm NTDS service is running:

```
powershell
CopyEdit
Get-Service NTDS
```

If not:

```
powershell
CopyEdit
Start-Service NTDS
```

3. Check registry permissions:

- o Run regedit
- o Navigate to:

```
sql
CopyEdit
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS
```

- o Right-click → Permissions → Ensure SYSTEM and Administrators have full control
-

### 3. NetLogons Test – “User credentials does not have permission...”

**Root Cause:** Either your account lacks "Access this computer from the network" rights or SYSVOL/Netlogon shares are not authenticating correctly.

#### **Fix:**

1. Run `secpol.msc`

- o Go to:

```
sql
CopyEdit
Local Policies → User Rights Assignment
```

- o Find:

- **Access this computer from the network**
- Ensure the following are present:
  - Administrators
  - Authenticated Users
  - Domain Admins

2. Restart Netlogon:

```
powershell
CopyEdit
net stop netlogon
net start netlogon
```

3. Force re-registration of SRV records:

```
powershell
CopyEdit
nltest /dsregdns
```

---

### 4. DFS Replication Test – Event ID 0xC00004B2, Error 160

**Root Cause:** DFSR can't contact a now-dead domain controller (probably WIN2016DC3) or the config still references it.

#### **Fix:**

1. Open `dfsmanagement.msc`

- o Expand **Replication** → SYSVOL
- o Ensure only WIN2016DC2 is a member
- o Remove any lingering connection/member pointing to WIN2016DC3

2. Manually trigger DFS config polling:

```
powershell
```

```
CopyEdit
dfsrdiag pollad
dfsrdiag backlog /rname:"Domain System Volume" /partner:WIN2016DC2
/rfname:SYSVOL
```

### 3. If unresolved:

- o Check:

```
ini
CopyEdit
CN=DFSR-LocalSettings,CN=WIN2016DC2,CN=Servers,...
```

in **ADSIEdit** and remove old connections.

---

## 5. SystemLog Errors – DNS, DCOM, WinRM, Group Policy

These are mostly symptoms, not causes. Here's how to clean them up:

### DNS Registration Errors

- Run:

```
powershell
CopyEdit
ipconfig /registerdns
nltest /dsregdns
```

- Restart DNS and Netlogon:

```
powershell
CopyEdit
net stop netlogon && net start netlogon
net stop dns && net start dns
```

### Group Policy Failures (Event ID 0x469)

- Make sure the network adapter has a valid IP, DNS points to 127.0.0.1 or local DC
- Force a group policy update:

```
powershell
CopyEdit
gpupdate /force
```

### DCOM/WinRM Errors

- Run:

```
cmd
CopyEdit
winrm quickconfig -q
netsh http add urlacl url=http://+:80/wsman/ user="NT AUTHORITY\NETWORK SERVICE"
```

- Also reset SPNs:

```
cmd
CopyEdit
setspn -R win2016dc2
```

---

## ✓ AFTER FIXING: RETEST AD HEALTH

```
dcdiag /v /c /e /f:"%userprofile%\Desktop\dcdiag_postfix.txt"
repadmin /replsummary
repadmin /showrepl
```

---

## ✓ Recommended: Schedule Cleanup and Reinforcement Tasks

Task	Command
Force DFSR Sync	<code>dfsrdiag pollad</code>
Reset Netlogon trust	<code>netdom resetpwd /server:WIN2016DC2 /user:administrator /passwordd:*</code>
Check all FSMO roles	<code>netdom query fsmo</code>
Check DNS health	<code>dcdiag /test:DNS</code>
Schedule DNS scavenging	Use DNS Manager GUI

---

Would you like a PowerShell script or .ps1 utility to:

- Reset services
- Fix DFSR and Netlogon
- Re-register DNS
- Check FSMO and replication status

Let me know, and I'll build a cleanup-and-validate script for you.

Here is a full-featured **PowerShell cleanup-and-validation script** specifically designed for a **post-domain controller recovery** scenario like yours. It restarts critical services, fixes DNS, validates replication, tests SYSVOL, and confirms FSMO roles.

---

## Features of the Script

- Restarts key services: Netlogon, DNS, W32Time, DFSR
- Re-registers DNS records
- Validates replication and NTDS health
- Checks SYSVOL/Netlogon shares
- Verifies FSMO role ownership
- Saves a detailed dcdiag report to the desktop

---

## Script: `PostRecovery-ADCleanup.ps1`

```
powershell
CopyEdit
<#
.SYNOPSIS
    Post-Recovery Active Directory Cleanup and Validation Script

.DESCRIPTION
    Designed for use after removing or losing a failed Domain Controller.
    It resets services, repairs DNS and DFSR issues, and validates the
    remaining DC.
#>

Write-Host "Starting Domain Controller Post-Recovery Cleanup" -ForegroundColor
Cyan

# Step 1: Restart essential services
$services = "Netlogon", "DNS", "DFSR", "W32Time"
foreach ($svc in $services) {
    Write-Host "Restarting $svc..." -ForegroundColor Yellow
    try {
        Restart-Service -Name $svc -ErrorAction Stop
    } catch {
        Write-Host "Failed to restart $svc: $_" -ForegroundColor Red
    }
}

# Step 2: Re-register DNS and SYSVOL
Write-Host "Re-registering DNS and restarting Netlogon for dynamic updates..."
-ForegroundColor Cyan
ipconfig /registerdns
nltest /dsregdns
Start-Sleep -Seconds 5

# Step 3: Force Group Policy update and DFSR poll
gpupdate /force
dfsrdiag pollad
```

```

# Step 4: Validate replication status
Write-Host "`nChecking replication summary..." -ForegroundColor Cyan
repadmin /replsummary

Write-Host "`nChecking individual replication partners..." -ForegroundColor
Cyan
repadmin /showrepl *

# Step 5: FSMO Roles validation
Write-Host "`nFSMO Role Holders:" -ForegroundColor Cyan
netdom query fsmo

# Step 6: Check SYSVOL and NETLOGON shares
Write-Host "`nVerifying SYSVOL and NETLOGON shares..." -ForegroundColor Cyan
Test-Path \\$env:COMPUTERNAME\SYSVOL | Out-Host
Test-Path \\$env:COMPUTERNAME\NETLOGON | Out-Host

# Step 7: Run DCDIAG and save to Desktop
$dcdiagPath = "$env:USERPROFILE\Desktop\dcdiag_postfix.txt"
Write-Host "`nRunning full DCDIAG scan... Please wait." -ForegroundColor Yellow
dcdiag /v /c /e /f:$dcdiagPath

Write-Host "`nDCDIAG completed. Results saved to:" -ForegroundColor Green
Write-Host $dcdiagPath -ForegroundColor White

Write-Host "`n✅ Active Directory cleanup script completed." -ForegroundColor
Green

```

---

## How to Use

1. Save as: PostRecovery-ADCleanup.ps1
2. Right-click PowerShell → **Run as Administrator**
3. Execute the script:

```



powershell
CopyEdit
Set-ExecutionPolicy RemoteSigned -Scope Process
.\PostRecovery-ADCleanup.ps1

```

---

Would you like an advanced version that also:

- Checks for lingering objects
  - Compares replication topology to expected state
  - Emails results or writes to a central log share?
  - **Your PowerShell environment is locked down by Group Policy**, so even if you try Set-ExecutionPolicy, it's overridden.
  - **Your system enforces a "signed scripts only" policy**, meaning **unsigned scripts** (like the .ps1 you're trying to run) are **blocked**.
  - This behavior is typical in:
    - **Domain-joined systems**
    - **Servers with security baselines**
    - **Environments with GPOs enforcing AllSigned or RemoteSigned globally**
    -
  - **✅ Solution: Use Inline Execution to Bypass the Policy**
-

- You can **execute the contents of the script inline** instead of calling the file directly.
-  **Step 1: Copy the contents of PostRecovery-ADCleanup.ps1**
- Paste it into a new elevated PowerShell window **manually** OR...
-  **Step 2: Use Invoke-Command to run the script inline:**
- powershell
- CopyEdit
- Invoke-Command -ScriptBlock {
- # Restart critical services
- \$services = "Netlogon", "DNS", "DFSR", "W32Time"
- foreach (\$svc in \$services) {
- Write-Host "Restarting \$svc..."
- try {
- Restart-Service -Name \$svc -ErrorAction Stop
- } catch {
- Write-Host ("Failed to restart {0}: `n{1}" -f \$svc, \$\_.Exception.Message) -ForegroundColor Red
- }
- }
- # DNS re-registration
- ipconfig /registerdns
- nltest /dsregdns
- 
- # Force policy and DFSR update
- gpupdate /force
- dfsrdiag pollad
- 
- # Replication and FSMO checks
- repadmin /replsummary
- repadmin /showrepl \*
- netdom query fsmo
- 
- # Check SYSVOL and Netlogon shares
- Test-Path \\\$env:COMPUTERNAME\SYSVOL | Out-Host
- Test-Path \\\$env:COMPUTERNAME\NETLOGON | Out-Host
- 
- # DCdiag output to Desktop
- dcdiag /v /c /e /f:"\$env:USERPROFILE\Desktop\dcdiag\_postfix.txt"
- }
- This avoids script file execution and **bypasses signing enforcement**.

```
PS C:\Windows\system32> Invoke-Command -ScriptBlock { >> # Restart critical services >> $services = "Netlogon", "DNS", "DFSR", "W32Time" >> foreach ($svc in $services) { >> Write-Host "Restarting $svc..." >> try { >> Restart-Service -Name $svc -ErrorAction Stop >> } catch { >> Write-Host ("Failed to restart {0}: n{1}" -f $svc, $_.Exception.Message) -ForegroundColor Red >> } >> >> # DNS re-registration >> ipconfig /registerdns >> nltest /dsregdns >> >> # Force policy and DFSR update >> gpupdate /force >> dfsrdiag pollad >> >> # Replication and FSMO checks >> repadmin /replsummary >> repadmin /showrepl * >> netdom query fsmo >> >> # Check SYSVOL and Netlogon shares >> Test-Path \\$env:COMPUTERNAME\SYSVOL | Out-Host >> Test-Path \\$env:COMPUTERNAME\NETLOGON | Out-Host >> >> # DCdiag output to Desktop >> dcdiag /v /c /e /f:"$env:USERPROFILE\Desktop\dcdiag_postfix.txt" >> } Restarting Netlogon... WARNING: Waiting for service 'Netlogon' to start... Restarting DNS... Restarting DFSR... Restarting W32Time... Windows IP Configuration Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes. Flags: 0 Connection Status = 0 0x0 NERR_Success The command completed successfully Updating policy... Computer Policy update has completed successfully. User Policy update has completed successfully. Operation Succeeded Replication Summary Start Time: 2025-06-19 09:37:47 Beginning data collection for replication summary, this may take awhile: .... Source DSA largest delta fails/total %% error Destination DSA largest delta fails/total %% error Repadmin: running command /showrepl against full DC Win2016DC2.HomeLab.TechSavvyProductions.com HQ-Homelab\WIN2016DC2 DSA Options: IS_GC Site Options: (none) DSA object GUID: 60228dba-cbc8-4304-868a-28f53a302f46 DSA invocationID: 7a35f1f8-1dce-4399-9264-25fdb678ef21 Schema master Win2016DC2.HomeLab.TechSavvyProductions.com Domain naming master Win2016DC2.HomeLab.TechSavvyProductions.com PDC Win2016DC2.HomeLab.TechSavvyProductions.com RID pool manager Win2016DC2.HomeLab.TechSavvyProductions.com Infrastructure master Win2016DC2.HomeLab.TechSavvyProductions.com The command completed successfully. True True
```

 **Success!** Your inline cleanup-and-validation PowerShell script **ran perfectly** and confirms:

---

## Summary of Results


### ◆ Services Restarted:

-  Netlogon
-  DNS
-  DFSR
-  W32Time


### ◆ DNS & SYSVOL

-  DNS resource records re-registered
-  \\WIN2016DC2\SYSVOL and \\WIN2016DC2\NETLOGON confirmed accessible (True, True)

### ◆ Group Policy

-  gpupdate completed successfully for both computer and user policy

### ◆ DFS Replication Config

-  dfsrdiag pollad succeeded

### ◆ FSMO Role Holders

All 5 FSMO roles are now held by:




Win2016DC2.HomeLab.TechSavvyProductions.com


### ◆ Replication Status

- No current partners = expected if only 1 DC remains
- No replication errors reported

---

## Next Recommended Steps

1.  **Open dcdiag\_postfix.txt** on your Desktop  
(This contains the full AD health check report)
2.  If you plan to add a new DC:
  - o Run: `dcpromo` OR `Install-ADDSDomainController`
  - o Allow SYSVOL and DFS replication to sync
3.  Clean DNS:

- o Remove stale records for the failed `win2016dc3`
  - o Use `dnsmgmt.msc` and clean up `_msdcs`, `_sites`, etc.
4.  Optionally audit ACLs:
- o Especially on `CN=NTDS Settings` to ensure no orphaned permissions
- 

## Bonus Offer

Would you like a follow-up script to:

-  Automatically clean **stale DNS and SRV records**
-  Check and remove **lingering objects**
-  Email or log status reports to a file share or admin inbox?

Let me know how you want to enhance this further. You're nearly done recovering from the failed DC!

Here is a complete **step-by-step guide** to **seize FSMO roles** to a surviving Windows Server 2016 domain controller (`win2016dc2`), **remove the failed DC** (`win2016dc3`) from Active Directory, and **validate the AD health** afterward.


---

## Layman's View

You had two computers that shared the job of managing your network. One broke, and the backup didn't work. Now, you're going to:

1. Move all critical management responsibilities to the one that still works.
  2. Remove the broken one from the list so your network doesn't keep looking for it.
  3. Check everything to make sure your network is healthy.
- 

## Technical Steps: Seize FSMO, Remove DC, and Validate AD Health

 Ensure `win2016dc2` is **fully updated**, has **correct DNS**, and **replication is healthy** before proceeding.

---

### ◆ STEP 1: Check FSMO Role Holders

Open PowerShell or Command Prompt as **Administrator** on win2016dc2:

```
powershell
CopyEdit
netdom query fsmo
```

If any FSMO roles are still assigned to the failed DC (win2016dc3), continue.

---

### ◆ **STEP 2: Seize FSMO Roles to win2016dc2**

Open PowerShell as **Administrator** on win2016dc2:

```
powershell
CopyEdit
# Import AD module
Import-Module ActiveDirectory

# Seize all 5 FSMO roles
Move-ADDirectoryServerOperationMasterRole -Identity win2016dc2
-OperationMasterRole SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster,
InfrastructureMaster -Force
```

 **Output should confirm the role transfer.**

 -Force is required to **seize** roles if the current holder is offline.

---

### ◆ **STEP 3: Verify FSMO Roles**

```
powershell
CopyEdit
netdom query fsmo
```

You should now see all FSMO roles assigned to win2016dc2.

---

### ◆ **STEP 4: Remove Failed DC (win2016dc3) from Active Directory**

#### **a) Manually Remove Metadata**

Run **ntdsutil**:

```
shell
CopyEdit
ntdsutil
```

Then inside the shell:

```
plaintext
CopyEdit
metadata cleanup
connections
connect to server win2016dc2
quit
select operation target
list domains
select domain <number>
list sites
select site <number>
list servers in site
select server <number> ← Select `win2016dc3`
quit
remove selected server
```

Confirm when asked to remove metadata.

---

## ◆ STEP 5: Clean DNS & Sites and Services

### a) Remove from DNS

In `dnsmgmt.msc`, delete:

- **A records** for `win2016dc3`
- **SRV records** under `_msdcs` and `_sites`

### b) Remove from Active Directory Sites and Services

1. Open `dssite.msc`
2. Expand the correct site.
3. Delete the **Server object** for `win2016dc3`, if still present.

---

## ◆ STEP 6: Add a New Domain Controller

On a new Windows Server:

1. Join to the domain.
2. Run:

```
powershell
```

```
CopyEdit
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

### 3. Promote it:

```
powershell
CopyEdit
Install-ADDSDomainController -DomainName "yourdomain.local" -InstallDNS
-Credential (Get-Credential)
```

### 4. Restart when prompted.

---

## ◆ STEP 7: Validate AD Health

### a) Replication Health

```
powershell
CopyEdit
repadmin /replsummary
repadmin /showrepl
```

Look for zero fails.

### b) Check Domain Health

```
powershell
CopyEdit
dcdiag /v /c /e /f:"%userprofile%\Desktop\dcdiag.txt"
```

Review the generated dcdiag.txt on your desktop.

### c) Verify DNS Health

```
powershell
CopyEdit
dnslint /ad /s localhost
```

---

## ◆ STEP 8: Optional – Demote if Needed

If any broken reference remains, forcibly remove it:

```
powershell
CopyEdit
Remove-ADObject -Identity "CN=win2016dc3,OU=Domain
Controllers,DC=yourdomain,DC=local" -Recursive
```

Use caution — verify the DistinguishedName with Get-ADObject.

---

## Sources

- [Microsoft Docs – FSMO Role Seizure](#)
- [AD DS Metadata Cleanup](#)
- [Readmin Reference](#)

---

Would you like a PowerShell script that wraps all tests (FSMO check, DCDiag, Readmin) for post-cleanup health validation?

### You said:

```
Move-ADDirectoryServerOperationMasterRole : Access is denied At line:1 char:1 +
Move-ADDirectoryServerOperationMasterRole -Identity win2016dc2 -Opera ... +
~~~~~+
CategoryInfo          : NotSpecified: (win2016dc2:ADDirectoryServer)
[Move-ADDirector...ationMasterRole], ADExce ption + FullyQualifiedErrorId :
ActiveDirectoryServer:0,Microsoft.ActiveDirectory.Management.Commands.MoveADDirectory
Ser verOperationMasterRole
```

### ChatGPT said:

The Access is denied error when running:

```
powershell
CopyEdit
Move-ADDirectoryServerOperationMasterRole -Identity win2016dc2 ...
```

means the account you're using **does not have the required permissions** to seize FSMO roles — especially **Schema Master** and **Domain Naming Master**, which require **Enterprise Admin** rights.

---

## Fix the “Access is denied” Issue — Step-by-Step

### ◆ Step 1: Log in with an Enterprise Admin Account

- Make sure you are **logged in as a user** who is a member of:
  - Enterprise Admins
  - Domain Admins
  - Schema Admins (*only needed if moving the Schema Master*)

⚠ If you're unsure, run:

```
powershell
CopyEdit
whoami
net user <yourusername> /domain
```

Check group membership includes:

- Enterprise Admins
  - Domain Admins
  - Schema Admins (*optional but preferred*)
- 

## ◆ Step 2: Run PowerShell as Administrator

Even with the right account, you need to:

- Right-click on PowerShell → **"Run as Administrator"**

Then run:

```
powershell
CopyEdit
Import-Module ActiveDirectory

Move-ADDirectoryServerOperationMasterRole -Identity win2016dc2
-OperationMasterRole 0,1,2,3,4 -Force
```

0-4 refers to all FSMO roles (SchemaMaster, DomainNamingMaster, RIDMaster, PDCEmulator, InfrastructureMaster)

---

## ◆ Step 3: If That Still Fails — Use NTDSUTIL

1. Open Command Prompt as Administrator
2. Type:

```
cmd
CopyEdit
ntdsutil
roles
connections
connect to server win2016dc2
quit
seize schema master
seize naming master
seize RID master
```

```
seize PDC
seize infrastructure master
quit
quit
```

✓ This forcibly transfers each FSMO role to win2016dc2.

---

## Validate the Transfer

```
powershell
CopyEdit
netdom query fsmo
```

---

## Important Notes

- You **only seize FSMO roles** if the original DC (win2016dc3) is **permanently offline** and will **never return**.
- **Do not** bring win2016dc3 back online after seizing roles unless it's **rebuilt or isolated**.

Would you like a PowerShell snippet to verify your user is a member of Enterprise Admins before trying again?

### You said:

Attempting safe transfer of schema FSMO before seizure. ldap\_modify\_sW error 0x32(50 (Insufficient Rights). Ldap extended error message is 00002098: SecErr: DSID-03152D12, problem 4003 (INSUFF\_ACCESS\_RIGHTS), data 0 Win32 error returned is 0x2098(Insufficient access rights to perform the operation.) ) Depending on the error code this may indicate a connection, ldap, or role transfer error. Transfer of schema FSMO failed, proceeding with seizure ... ldap\_modify of SD failed with 0x32(50 (Insufficient Rights). Ldap extended error message is 00000005: SecErr: DSID-03152DB2, problem 4003 (INSUFF\_ACCESS\_RIGHTS), data 0 Win32 error returned is 0x5(Access is denied.)

### ChatGPT said:

You're seeing **LDAP error 0x32 (INSUFF\_ACCESS\_RIGHTS)** and **Win32 error 0x5 (Access is denied)** while attempting to **seize the Schema Master FSMO role** — this is one of the most permission-sensitive roles in Active Directory.

These errors mean the currently logged-in user **does not have sufficient privileges** in the **forest schema**, specifically **not a member of the Schema Admins group**.

---

## ✓ Fix: Grant Your Account Schema Admin Permissions

### ◆ Step 1: Add Your Account to the Schema Admins Group

1. Log in to `win2016dc2` as a **Domain Admin or Enterprise Admin**.
2. Open **Active Directory Users and Computers** (`dsa.msc`)
3. Enable **Advanced Features**:  
View → Advanced Features
4. Navigate to:

```
ini
CopyEdit
CN=Users, DC=yourdomain, DC=local
```

5. Locate the group:

```
graphql
CopyEdit
Schema Admins
```

6. Add your user account to that group.

💡 Alternatively, use PowerShell:

```
powershell
CopyEdit
Add-ADGroupMember -Identity "Schema Admins" -Members "YourUsername"
```

---

### ◆ Step 2: Log Off and Back On

Group membership changes **don't take effect until re-login**. So:

- **Log off** the session.
  - **Log back in** with the same user.
  - Run PowerShell again **as Administrator**.
- 

### ◆ Step 3: Retry Seizure (If Needed)

Now, re-run:

```
cmd
CopyEdit
ntdsutil
roles
connections
```

```
connect to server win2016dc2
quit
seize schema master
```

Or use:

```
powershell
CopyEdit
Move-ADDirectoryServerOperationMasterRole -Identity win2016dc2
-OperationMasterRole SchemaMaster -Force
```

---

## **Optional: Remove Yourself from Schema Admins**

Once FSMO roles are successfully seized, for security:

```
powershell
CopyEdit
Remove-ADGroupMember -Identity "Schema Admins" -Members "YourUsername"
-Confirm:$false
```

---

### **Validate**

```
powershell
CopyEdit
netdom query fsmo
```

Make sure all roles are now held by win2016dc2.

---

## **Would You Like a Full Script to:**

- Check your account group memberships
- Prompt you to add to Schema Admins if not found
- Log changes and test FSMO role ownership?

Let me know, and I'll generate it for you.

**You said:**

How to lift the accidental deletion feature in AD temporarily remove Win2016dc3 from "sites and services"

**ChatGPT said:**

To temporarily disable "Protect object from accidental deletion" in Active Directory for a domain controller (e.g., win2016dc3) so you can manually delete it from **Active Directory Sites and Services**, follow these steps:

---

## ◆ Why This Is Needed

By default, when you promote a Domain Controller, the "**Protect object from accidental deletion**" checkbox is **enabled** on its AD object. This prevents you from deleting the server or NTDS settings from Sites and Services.

---

## ✔ Step-by-Step: Lift Accidental Deletion Protection

### 🔧 Method 1: Using GUI (ADUC – Active Directory Users and Computers)

1. On win2016dc2, open:

```
CopyEdit  
dsa.msc
```

2. Go to **View** →  **Advanced Features**
3. Navigate to:

```
mathematica  
CopyEdit  
Active Directory Users and Computers > Domain Controllers
```

4. Right-click the object win2016dc3, and select **Properties**
5. Go to the **Object** tab
6. Uncheck:

```
csharp  
CopyEdit  
✔ Protect object from accidental deletion
```

7. Click **OK**
- 

### 🔧 Method 2: Using PowerShell

Run as Administrator:

```
powershell
CopyEdit
# Get the distinguished name of Win2016dc3
Get-ADObject -Filter 'Name -eq "Win2016dc3"' -Properties DistinguishedName

# Disable accidental deletion protection
Set-ADObject -Identity "CN=Win2016dc3,OU=Domain
Controllers,DC=yourdomain,DC=local" -ProtectedFromAccidentalDeletion $false
```

Replace the DN with the exact value from your environment.

---

## ▼ Then Remove from AD Sites and Services

1. Open:

```
CopyEdit
dssite.msc
```

2. Expand the correct **Site** → **Servers**
  3. Locate Win2016dc3
  4. Delete the:
    - o **NTDS Settings** first (if present)
    - o Then the **Server object**
- 

## ✓ Final Validation

After deletion, make sure there are no replication links referencing Win2016dc3:

```
powershell
CopyEdit
repadmin /replsummary
repadmin /showrepl
```

Also verify DNS:

```
powershell
CopyEdit
dnscmd /enumrecords yourdomain.local _msdcs.yourdomain.local /type A
```

Delete leftover entries in:

- Forward Lookup Zones
- Reverse Lookup Zones

---

Let me know if you'd like to **script the detection and cleanup** of all leftover records (DNS, metadata, replication links).

**You said:**

I am unable to remove win2016dc3 from the "Servers" object in AD sites and services

**ChatGPT said:**

If you're unable to remove win2016dc3 from "**Servers**" in **Active Directory Sites and Services**, even after lifting accidental deletion protection, it's likely due to lingering **NTDS Settings**, **permissions**, or **replication metadata** still being intact. Here's how to resolve this step-by-step:

---

## **Step-by-Step: Forcibly Remove Domain Controller from Sites and Services**

### **Prerequisites**

Make sure:

- You have **Domain Admin** and **Enterprise Admin** rights
- You've logged in to **win2016dc2**
- Accidental deletion protection is disabled

---

### ♦ **Step 1: Open ADSI Edit (Advanced Manual Cleanup)**

1. Run:

```
shell
CopyEdit
adsiedit.msc
```

2. Right-click **ADSI Edit > Connect to...**

- o Select: Configuration naming context
- o Click OK

3. Navigate to:

```
ini
CopyEdit
CN= Sites > CN=<YourSiteName> > CN=Servers > CN=win2016dc3
```

Inside you'll likely see:

- o CN=NTDS Settings
- o Possibly additional sub-objects

---

### ◆ Step 2: Delete NTDS Settings First

1. Right-click **CN=NTDS Settings**
2. Click **Delete**
  - o Confirm any warnings

Then:

3. Right-click **CN=win2016dc3** → **Delete**

---

### ◆ Step 3: Use `ntdsutil` for Metadata Cleanup (Recommended after ADSI edit)

1. Open **Command Prompt as Administrator**
2. Run:

```
cmd
CopyEdit
ntdsutil
metadata cleanup
connections
connect to server win2016dc2
quit
select operation target
list domains
select domain <yourdomain#>
list sites
select site <yoursite#>
list servers in site
select server <win2016dc3#>
quit
remove selected server
quit
```

✓ This will **fully remove all references** to win2016dc3.

---

### ◆ Step 4: Remove Remaining DNS Records

Open `dnsmgmt.msc`:

- Look under:

```
lua
CopyEdit
_msdcg.yourdomain.local
_sites
_tcp
_udp
```

- Delete all SRV and A records pointing to win2016dc3

Also check:

- **Forward Lookup Zone** (A record)
  - **Reverse Lookup Zone** (PTR record)
- 

## ◆ Step 5: Confirm Cleanup

### Replication

```
powershell
CopyEdit
repadmin /replsummary
repadmin /showrepl
```

### FSMO Roles

```
powershell
CopyEdit
netdom query fsmo
```

### Global Catalogs

```
nltest /dclist:yourdomain.local
```

### AD Health

```
dcdiag /v /c /e /f:"%userprofile%\Desktop\dcdiag.txt"
```

---

## If You Still Cannot Delete

If ADSI Edit and `ntdsutil` both **fail to delete the Server object**, likely causes include:

- ACL corruption
- Replication delay (wait for replication to complete)

- Object ownership issues

Let me know and I can provide:

- ✓ A script to take **ownership and force-delete** the object from AD
- ✓ A tool-based method using **LDP.exe** or **PowerShell/ADSI COM**

Would you like the script or PowerShell command to force ownership and delete the object?

**You said:**

Running dcdiag I received the following failures or errors as shown below, give step by step guide to troubleshooting each error or failure in the dcdiag report, this report is after a recovery of a failed domain controller that had to be manually removed from AD. Starting test: Services \* Checking Service: EventSystem \* Checking Service: RpcSs \* Checking Service: NTDS Could not open NTDS Service on WIN2016DC2, error 0x5 "Access is denied." Starting test: Replications \* Replications Check [Replications Check,WIN2016DC2] DsReplicaGetInfo(PENDING\_OPS, NULL) failed, error 0x2105 "Replication access was denied." ..... WIN2016DC2 failed test Replications Starting test: NetLogons \* Network Logons Privileges Check Verified share \\WIN2016DC2\netlogon Verified share \\WIN2016DC2\sysvol [WIN2016DC2] User credentials does not have permission to perform this operation. The account used for this test must have network logon privileges for this machine's domain. .... WIN2016DC2 failed test NetLogons Starting test: Intersite Doing intersite inbound replication test on site HQ-Homelab: Locating & Contacting Intersite Topology Generator (ISTG) ... The ISTG for site HQ-Homelab is: WIN2016DC2. \*\*\*Error: On server WIN2016DC2, DsReplicaGetInfo() failed, error: 0x2105 "Replication access was denied." Inbound intersite replication test cannot proceed. Skipping site Mikrotek, this site is outside the scope provided by the command line arguments provided. .... HomeLab.TechSavvyProductions.com failed test Intersite

**ChatGPT said:**

You're seeing a **common post-cleanup issue** after manually removing a failed DC: the surviving DC (WIN2016DC2) is showing **permission-related DCdiag failures** for services, replication, and network logon privileges. These failures are often due to:

- Incomplete cleanup of the demoted/removed DC.
- Lack of **elevated permissions** for the account running DCdiag.
- Damaged **DC-level ACLs, missing group memberships, or SYSVOL inconsistencies.**

Below is a **step-by-step diagnostic and fix guide for each error** you posted:

---

 **Test:** `services`

**Error:**

Could not open NTDS Service on WIN2016DC2, error 0x5 "Access is denied."

### **Fix:**

This is likely because you're running `dcdiag` without elevated privileges or from a **non-Domain Admin** account.

### **Steps:**

1. **Log in as a Domain Admin** (or equivalent admin account).
2. Open **Command Prompt or PowerShell as Administrator**.
3. Rerun `dcdiag`:

```
dcdiag /v /c /e /f:"%userprofile%\Desktop\dcdiag.txt"
```

If the error persists:

4. Verify your user is a member of:

```
whoami  
net user %username% /domain
```

Ensure you're in:

- Domain Admins
  - Enterprise Admins
- 

### **Test:** Replications

**Error:**

DsReplicaGetInfo(PENDING\_OPS, NULL) failed, error 0x2105 — Replication access was denied.

### **Fix:**

This error means that the current user does **not have permission to query** AD replication metadata.

### **Steps:**

1. Ensure you're running as a member of Domain Admins.
2. Ensure the **NTDS Settings object** ACL is intact:

**Using ADSIEdit:**

- adsiedit.msc
- Connect to: **Configuration**
- Go to:

```
ini
CopyEdit
CN=Sites > CN=HQ-Homelab > CN=Servers > CN=WIN2016DC2 > CN=NTDS Settings
```

- Right-click CN=NTDS Settings → Properties → **Security**
- Ensure your user (or Domain Admins group) has **Read/Write/Replicate Directory Changes** permissions.

### 3. Force reset ACLs (use with caution):

```
powershell
CopyEdit
dsaclS "CN=NTDS
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=ho
melab,DC=techsavvyproductions,DC=com" /I:T /G "Domain Admins:GA"
```

### 4. Restart NTDS:

```
powershell
CopyEdit
net stop ntds
net start ntds
```

## **Test:** NetLogons

### **Error:**

User credentials does not have permission to perform this operation.

### **Fix:**

This is a **missing or broken trust between DC and domain**, usually tied to:

- Broken Netlogon service
- Computer account trust problems
- SYSVOL/NETLOGON share permission issues

### **Steps:**

#### 1. Ensure Netlogon and NTFRS or DFS-R services are running:

```
powershell
CopyEdit
```

```
Get-Service Netlogon, NTFRS, DFSR
```

Start them if stopped:

```
powershell  
CopyEdit  
Start-Service Netlogon
```

2. Verify `\\WIN2016DC2\NETLOGON` and `\\WIN2016DC2\SYSVOL` are shared and accessible:
  - o From another machine:

```
cmd  
CopyEdit  
net use \\WIN2016DC2\netlogon
```

3. Confirm machine trust account is not broken:

```
powershell  
CopyEdit  
nltest /sc_verify:homelab.techsavvyproductions.com
```

If trust is broken:

```
powershell  
CopyEdit  
netdom resetpwd /server:WIN2016DC2 /userd:administrator /passwordd:*
```

Then restart Netlogon.

---

## **Test:** Intersite

**Error:**

DsReplicaGetInfo() failed, error: 0x2105 — Replication access was denied.

## **Fix:**

Same root cause as the **Replications** test — permissions missing or corrupted ACLs.

## **Steps:**

1. Double-check the **ISTG role** is held by WIN2016DC2:

```
powershell  
CopyEdit
```

```
Get-ADObject -Filter {objectClass -eq "nTDSDSA"} -SearchBase "CN=NTDS
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=ho
melab,DC=techsavvyproductions,DC=com" -Properties * | Select-Object
interSiteTopologyGenerator
```

## 2. If ISTG is not working:

- o Re-register it:

```
powershell
CopyEdit
repadmin /rehost <SiteName>
```

## 3. Clean stale connections manually from dssite.msc or use:

```
powershell
CopyEdit
repadmin /removelingerobjects WIN2016DC2
"dc=homelab,dc=techsavvyproductions,dc=com" /advisory_mode
```

If safe:

```
powershell
CopyEdit
repadmin /removelingerobjects WIN2016DC2
"dc=homelab,dc=techsavvyproductions,dc=com"
```

---

## Post-Fix Verification

After applying all fixes, rerun:

```
cmd
CopyEdit
dcdiag /v /c /e /f:"%userprofile%\Desktop\dcdiag-clean.txt"
```

Also run:

```
powershell
CopyEdit
repadmin /replsummary
repadmin /showrepl
```

Check:

- No replication failures
  - SYSVOL is accessible
  - DNS is resolving correctly
-



## Optional Tools

Tool	Purpose
<b>Readmin</b>	Check replication health, force replication
<b>ADSIEdit</b>	Manually inspect/repair AD objects and ACLs
<b>Dsacls</b>	View and modify AD permissions
<b>Netdom</b>	Repair trust and reset passwords
<b>Dcdiag</b>	Full AD health diagnostics

---

Would you like a **scripted checklist** or **PowerShell toolset** to run all these post-recovery checks automatically?

**You said:**

```
C : \Users\HomeBoss>dsacls "CN-NTOS Settings,
CN=WIN20160C2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN-Configuration, DCshomelab, 0
C=techsavvyproductions,OC=com" /I:T /G "Domain Admins:GA" Specified operation failed
with ldap error: 00000005: SecErr: OSID-03152082, problem 4003
(INSUFF_ACCESS_RIGHTS), data 0 Insufficient Rights Access is denied. The command failed
to complete successfully.
```

**ChatGPT said:**

You're getting this LDAP error when running `dsacls`:

```
pgsql
CopyEdit
INSUFF_ACCESS_RIGHTS (00000005) - Access is denied.
```

This typically happens when:

- Your user account **does not have adequate permissions** to modify the NTDS Settings object.
- You're **not a member of the correct admin groups**, or
- The **ACLs on the object are corrupted** (common after manual DC cleanup).
- Or — **the DN is malformed** (note: you're using `CN-NTOS Settings` instead of `CN=NTDS Settings`)



## Step-by-Step Fix for `Access is Denied` on NTDS Settings



### Step 1: Fix the DN Syntax (Critical)

Your DN is incorrect. This part:

```
CopyEdit
CN-NTOS Settings
```

Should be:

```
ini
CopyEdit
CN=NTDS Settings
```

Also:

```
mathematica
CopyEdit
DCshomelab, 0 C=techsavvyproductions,OC=com
```

Should be:

```
ini
CopyEdit
DC=homelab,DC=techsavvyproductions,DC=com
```

### **Corrected Command:**

```
powershell
CopyEdit
dsacIs "CN=NTDS
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=ho
melab,DC=techsavvyproductions,DC=com" /I:T /G "Domain Admins:GA"
```

---

## **Step 2: Ensure You Have Schema and Enterprise Admin Rights**

Verify you're logged in with a user that is a member of:

- Domain Admins
- Enterprise Admins
- Schema Admins (optional, but helpful in AD-integrated recovery scenarios)

Check with:

```
powershell
CopyEdit
whoami
net user %username% /domain
```

If your user is missing any of the above groups, **add the user**, then **log off and back on**.

---

### **Step 3: Take Ownership of NTDS Settings (if ACLs are broken)**


If ACLs are damaged, take ownership manually:

#### **a) Open `adsiedit.msc`**

1. Connect to **Configuration**
2. Navigate to:

```
ini
CopyEdit
CN=Sites > CN=HQ-Homelab > CN=Servers > CN=WIN2016DC2 > CN=NTDS Settings
```

3. Right-click **NTDS Settings > Properties > Security** tab
4. Click **Advanced**
5. Go to **Owner** tab
6. Change owner to **Domain Admins** or your user
7. Click OK and Apply until out of dialog boxes

 Reopen the Properties window, and now you should be able to **modify permissions**

---

### **Step 4: Retry the `dsac1s` Command**

Once ownership is changed:

```
powershell
CopyEdit
dsac1s "CN=NTDS
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=ho
melab,DC=techsavvyproductions,DC=com" /I:T /G "Domain Admins:GA"
```

---

### **Alternative (if `dsac1s` fails again): Use PowerShell to Set ACL**

Use this **PowerShell workaround** to set FullControl:

```
powershell
CopyEdit
$identity = "Domain Admins"
$objectDN = "CN=NTDS
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=ho
melab,DC=techsavvyproductions,DC=com"

$adObject = [ADSI]"LDAP://$objectDN"
$acl = $adObject.psbase.ObjectSecurity
```

```
$rule = New-Object
System.DirectoryServices.ActiveDirectoryAccessRule($identity,"GenericAll","Allow")
$acl.AddAccessRule($rule)
$adObject.psbase.ObjectSecurity = $acl
$adObject.CommitChanges()
```

---

## Final Steps: Retest After Fixes

Once you have permissions:

1. Run `repadmin /showrepl`
  2. Run `dcdiag /v /c /e /f:"%userprofile%\Desktop\dcdiag-clean.txt"`
  3. Confirm no more:
    - o Access is denied
    - o Replication access was denied
- 

Would you like a PowerShell script that **checks your FSMO roles, AD permissions, and offers repair actions** interactively?

**You said:**

This is the entire dcdiag test report: Directory Server Diagnosis Performing initial setup: Trying to find home server... \* Verifying that the local machine Win2016DC2, is a Directory Server. Home Server = Win2016DC2 \* Connecting to directory service on server Win2016DC2. \* Identified AD Forest. Collecting AD specific global data \* Collecting site info. Calling `ldap_search_init_page(hld,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com,LDAP_SCOPE_SUBTREE,(objectCategory=ntDSSiteSettings),.....` The previous call succeeded Iterating through the sites Looking at base site object: `CN=NTDS Site Settings,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com` Getting ISTG and options for the site Looking at base site object: `CN=NTDS Site Settings,CN=Mikrotek,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com` Getting ISTG and options for the site \* Identifying all servers. Calling `ldap_search_init_page(hld,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com,LDAP_SCOPE_SUBTREE,(objectClass=ntDSDsa),.....` The previous call succeeded.... The previous call succeeded Iterating through the list of servers Getting information for the server `CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com` objectGuid obtained InvocationID obtained dnsHostname obtained site info obtained All the info for the server collected \* Identifying all NC cross-refs. \* Found 1 DC(s). Testing 1 of them. Done gathering initial info. Doing initial required tests Testing server: `HQ-Homelab\WIN2016DC2` Starting test: Connectivity \* Active Directory LDAP Services Check Determining IP4 connectivity Determining IP6 connectivity \* Active Directory RPC Services Check ..... WIN2016DC2 passed test Connectivity Doing

primary tests Testing server: HQ-Homelab\WIN2016DC2 Starting test: Advertising The DC  
WIN2016DC2 is advertising itself as a DC and having a DS. The DC WIN2016DC2 is  
advertising as an LDAP server The DC WIN2016DC2 is advertising as having a writable  
directory The DC WIN2016DC2 is advertising as a Key Distribution Center The DC  
WIN2016DC2 is advertising as a time server The DS WIN2016DC2 is advertising as a GC.  
..... WIN2016DC2 passed test Advertising Starting test: CheckSecurityError \* Dr  
Auth: Beginning security errors check! Found KDC WIN2016DC2 for domain  
HomeLab.TechSavvyProductions.com in site HQ-Homelab Checking machine account for DC  
WIN2016DC2 on DC WIN2016DC2. \* SPN found  
:LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.c  
om \* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com \* SPN found  
:LDAP/WIN2016DC2 \* SPN found  
:LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB \* SPN found  
:LDAP/60228dba-cbc8-4304-868a-28f53a302f46.\_msdcs.HomeLab.TechSavvyProductions.com  
\* SPN found  
:E3514235-4B06-11D1-AB04-00C04FC2DCD2/60228dba-cbc8-4304-868a-28f53a302f46/Hom  
eLab.TechSavvyProductions.com \* SPN found  
:HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.c  
om \* SPN found :HOST/Win2016DC2.HomeLab.TechSavvyProductions.com \* SPN found  
:HOST/WIN2016DC2 \* SPN found  
:HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB \* SPN found  
:GC/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com  
[WIN2016DC2] DsReplicaGetInfo(KCC\_DS\_CONNECT\_FAILURES) failed with error 8453,  
Replication access was denied.. [WIN2016DC2] Unable to query the list of KCC connection  
failures. Continuing... [WIN2016DC2] No security related replication errors were found on this  
DC! To target the connection to a specific source DC use /ReplSource:<DC>. ....  
WIN2016DC2 passed test CheckSecurityError Starting test: CutoffServers \* Configuration  
Topology Aliveness Check \* Analyzing the alive system replication topology for  
DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing  
upstream (of target) analysis. \* Performing downstream (of target) analysis. \* Analyzing the  
alive system replication topology for  
DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing  
upstream (of target) analysis. \* Performing downstream (of target) analysis. \* Analyzing the  
alive system replication topology for  
CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com. \*  
Performing upstream (of target) analysis. \* Performing downstream (of target) analysis. \*  
Analyzing the alive system replication topology for  
CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing upstream  
(of target) analysis. \* Performing downstream (of target) analysis. \* Analyzing the alive system  
replication topology for DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing  
upstream (of target) analysis. \* Performing downstream (of target) analysis. ....  
WIN2016DC2 passed test CutoffServers Starting test: FrsEvent \* The File Replication Service  
Event log test Skip the test because the server is running DFSR. .... WIN2016DC2  
passed test FrsEvent Starting test: DFSREvent The DFS Replication Event Log. There are  
warning or error events within the last 24 hours after the SYSVOL has been shared. Failing  
SYSVOL replication problems may cause Group Policy problems. An error event occurred.

EventID: 0xC00004B2 Time Generated: 06/19/2025 04:04:02 Event String: The DFS Replication service failed to contact domain controller to access configuration information. Replication is stopped. The service will try again during the next configuration polling cycle, which will occur in 60 minutes. This event can be caused by TCP/IP connectivity, firewall, Active Directory Domain Services, or DNS issues. Additional Information: Error: 160 (One or more arguments are not correct.) ..... WIN2016DC2 failed test DFSREvent Starting test: SysVolCheck \* The File Replication Service SYSVOL ready test File Replication Service's SYSVOL is ready ..... WIN2016DC2 passed test SysVolCheck Starting test: FrsSysVol \* The File Replication Service SYSVOL ready test File Replication Service's SYSVOL is ready ..... WIN2016DC2 passed test FrsSysVol Starting test: KccEvent \* The KCC Event log test Found no KCC errors in "Directory Service" Event log in the last 15 minutes. .... WIN2016DC2 passed test KccEvent Starting test: KnowsOfRoleHolders Role Schema Owner = CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com Role Domain Owner = CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com Role PDC Owner = CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com Role Rid Owner = CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com Role Infrastructure Update Owner = CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com ..... WIN2016DC2 passed test KnowsOfRoleHolders Starting test: MachineAccount Checking machine account for DC WIN2016DC2 on DC WIN2016DC2. \* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com \* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com \* SPN found :LDAP/WIN2016DC2 \* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB \* SPN found :LDAP/60228dba-cbc8-4304-868a-28f53a302f46.\_msdcs.HomeLab.TechSavvyProductions.com \* SPN found :E3514235-4B06-11D1-AB04-00C04FC2DCD2/60228dba-cbc8-4304-868a-28f53a302f46/HomeLab.TechSavvyProductions.com \* SPN found :HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com \* SPN found :HOST/Win2016DC2.HomeLab.TechSavvyProductions.com \* SPN found :HOST/WIN2016DC2 \* SPN found :HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB \* SPN found :GC/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com ..... WIN2016DC2 passed test MachineAccount Starting test: NCSecDesc \* Security Permissions check for all NC's on DC WIN2016DC2. \* Security Permissions Check for DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com (NDNC, Version 3) \* Security Permissions Check for DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com (NDNC, Version 3) \* Security Permissions Check for CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com (Schema, Version 3) \* Security Permissions Check for

CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com (Configuration,Version 3) \* Security Permissions Check for DC=HomeLab,DC=TechSavvyProductions,DC=com (Domain,Version 3) ..... WIN2016DC2 passed test NCSecDesc Starting test: NetLogons \* Network Logons Privileges Check Verified share \\WIN2016DC2\netlogon Verified share \\WIN2016DC2\sysvol [WIN2016DC2] User credentials does not have permission to perform this operation. The account used for this test must have network logon privileges for this machine's domain. .... WIN2016DC2 failed test NetLogons Starting test: ObjectsReplicated WIN2016DC2 is in domain DC=HomeLab,DC=TechSavvyProductions,DC=com Checking for CN=WIN2016DC2,OU=Domain Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com in domain DC=HomeLab,DC=TechSavvyProductions,DC=com on 1 servers Object is up-to-date on all servers. Checking for CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com in domain CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com on 1 servers Object is up-to-date on all servers. .... WIN2016DC2 passed test ObjectsReplicated Starting test: OutboundSecureChannels \* The Outbound Secure Channels test \*\* Did not run Outbound Secure Channels test because /testdomain: was not entered ..... WIN2016DC2 passed test OutboundSecureChannels Starting test: Replications \* Replications Check [Replications Check,WIN2016DC2] DsReplicaGetInfo(PENDING\_OPS, NULL) failed, error 0x2105 "Replication access was denied." ..... WIN2016DC2 failed test Replications Starting test: RidManager \* Available RID Pool for the Domain is 14600 to 1073741823 \* Win2016DC2.HomeLab.TechSavvyProductions.com is the RID Master \* DsBind with RID Master was successful \* rIDAllocationPool is 4100 to 4599 \* rIDPreviousAllocationPool is 4100 to 4599 \* rIDNextRID: 4101 ..... WIN2016DC2 passed test RidManager Starting test: Services \* Checking Service: EventSystem \* Checking Service: RpcSs \* Checking Service: NTDS Could not open NTDS Service on WIN2016DC2, error 0x5 "Access is denied." \* Checking Service: DnsCache \* Checking Service: DFSR \* Checking Service: IsmServ \* Checking Service: kdc \* Checking Service: SamSs \* Checking Service: LanmanServer \* Checking Service: LanmanWorkstation \* Checking Service: w32time \* Checking Service: NETLOGON ..... WIN2016DC2 failed test Services Starting test: SystemLog \* The System Event log test An error event occurred. EventID: 0x00002720 Time Generated: 06/19/2025 04:02:17 Event String: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {D63B10C5-BB46-4990-A94F-E40B9D520160} and APPID {9CA88EE3-ACB7-47C8-AFC4-AB702511C276} to the user HOMELAB\HomeBoss SID (S-1-5-21-3892272843-2021369796-1445886767-1103) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool. An error event occurred. EventID: 0x00000029 Time Generated: 06/19/2025 04:03:38 Event String: Hypervisor launch failed; Either VMX not present or not enabled in BIOS. A warning event occurred. EventID: 0x000000DB Time Generated: 06/19/2025 04:03:39 Event String: The driver \Driver\vmusb failed to load for the device ROOT\VMBus\0000. A warning event occurred. EventID: 0x80040020 Time Generated: 06/19/2025 04:03:39 Event String: The driver detected that the device \Device\Harddisk1\DR1 has its write cache enabled. Data corruption may occur. A

warning event occurred. EventID: 0x80040020 Time Generated: 06/19/2025 04:03:39 Event String: The driver detected that the device \Device\Harddisk1\DR1 has its write cache enabled. Data corruption may occur. A warning event occurred. EventID: 0x80040020 Time Generated: 06/19/2025 04:03:39 Event String: The driver detected that the device \Device\Harddisk1\DR1 has its write cache enabled. Data corruption may occur. A warning event occurred. EventID: 0x000003F6 Time Generated: 06/19/2025 04:03:43 Event String: Name resolution for the name \_ldap.\_tcp.dc.\_msdcs.HomeLab.TechSavvyProductions.com. timed out after none of the configured DNS servers responded. An error event occurred. EventID: 0x00000469 Time Generated: 06/19/2025 04:04:01 Event String: The processing of Group Policy failed because of lack of network connectivity to a domain controller. This may be a transient condition. A success message would be generated once the machine gets connected to the domain controller and Group Policy has successfully processed. If you do not see a success message for several hours, then contact your administrator. An error event occurred. EventID: 0x00000469 Time Generated: 06/19/2025 04:04:02 Event String: The processing of Group Policy failed because of lack of network connectivity to a domain controller. This may be a transient condition. A success message would be generated once the machine gets connected to the domain controller and Group Policy has successfully processed. If you do not see a success message for several hours, then contact your administrator. A warning event occurred. EventID: 0x00001796 Time Generated: 06/19/2025 04:04:13 Event String: Microsoft Windows Server has detected that NTLM authentication is presently being used between clients and this server. This event occurs once per boot of the server on the first time a client uses NTLM with this server. NTLM is a weaker authentication mechanism. Please check: Which applications are using NTLM authentication? Are there configuration issues preventing the use of stronger authentication such as Kerberos authentication? If NTLM must be supported, is Extended Protection configured? Details on how to complete these checks can be found at <http://go.microsoft.com/fwlink/?LinkId=225699>. An error event occurred. EventID: 0x00000469 Time Generated: 06/19/2025 04:04:15 Event String: The processing of Group Policy failed because of lack of network connectivity to a domain controller. This may be a transient condition. A success message would be generated once the machine gets connected to the domain controller and Group Policy has successfully processed. If you do not see a success message for several hours, then contact your administrator. An error event occurred. EventID: 0x00002720 Time Generated: 06/19/2025 04:04:15 Event String: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {8D8F4F83-3594-4F07-8369-FC3C3CAE4919} and APPID {F72671A9-012C-4725-9D2F-2A4D32D65169} to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool. An error event occurred. EventID: 0x00072790 Time Generated: 06/19/2025 04:04:19 Event String: The WinRM service is not listening for HTTP requests because there was a failure binding to the URL (http://+:80/wsman/) in HTTP.SYS. No remote requests will be serviced on that URL. User Action Please use "netsh http" to check if ACL for URL (http://+:80/wsman/) is set to Network Service. Additional Data The error code received from HTTP.sys is 5: %%5 A warning event occurred. EventID: 0x000727AA Time Generated: 06/19/2025 04:04:21 Event String: The WinRM service failed to create the following SPNs: WSMAN/Win2016DC2.HomeLab.TechSavvyProductions.com; WSMAN/Win2016DC2. Additional Data The error received was 1355: %%1355. User Action The SPNs can be created

by an administrator using setspn.exe utility. An error event occurred. EventID: 0x0000168E  
Time Generated: 06/19/2025 04:04:23 Event String: The dynamic registration of the DNS record  
'\_ldap.\_tcp.HomeLab.TechSavvyProductions.com. 600 IN SRV 0 100 389  
win2016dc2.homelab.techsavvyproductions.com.' failed on the following DNS server: DNS  
server IP address: :: Returned Response Code (RCODE): 0 Returned Status Code: 0 For  
computers and users to locate this domain controller, this record must be registered in DNS.  
USER ACTION Determine what might have caused this failure, resolve the problem, and initiate  
registration of the DNS records by the domain controller. To determine what might have caused  
this failure, run DCDiag.exe. To learn more about DCDiag.exe, see Help and Support Center. To  
initiate registration of the DNS records by this domain controller, run 'nltest.exe /dsregdns'  
from the command prompt on the domain controller or restart Net Logon service. Or, you can  
manually add this record to DNS, but it is not recommended. ADDITIONAL DATA Error Value:  
Bad DNS packet. An error event occurred. EventID: 0x00002720 Time Generated: 06/19/2025  
04:04:38 Event String: The application-specific permission settings do not grant Local  
Activation permission for the COM Server application with CLSID  
{D63B10C5-BB46-4990-A94F-E40B9D520160} and APPID  
{9CA88EE3-ACB7-47C8-AFC4-AB702511C276} to the user HOMELAB\HomeBoss SID  
(S-1-5-21-3892272843-2021369796-1445886767-1103) from address LocalHost (Using LRPC)  
running in the application container Unavailable SID (Unavailable). This security permission can  
be modified using the Component Services administrative tool. An error event occurred.  
EventID: 0x00002720 Time Generated: 06/19/2025 04:04:56 Event String: The  
application-specific permission settings do not grant Local Activation permission for the COM  
Server application with CLSID {D63B10C5-BB46-4990-A94F-E40B9D520160} and APPID  
{9CA88EE3-ACB7-47C8-AFC4-AB702511C276} to the user HOMELAB\HomeBoss SID  
(S-1-5-21-3892272843-2021369796-1445886767-1103) from address LocalHost (Using LRPC)  
running in the application container Unavailable SID (Unavailable). This security permission can  
be modified using the Component Services administrative tool. An error event occurred.  
EventID: 0x0000272C Time Generated: 06/19/2025 04:14:19 Event String: DCOM was unable  
to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any  
of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).  
An error event occurred. EventID: 0x0000272C Time Generated: 06/19/2025 04:14:19 Event  
String: DCOM was unable to communicate with the computer  
zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols;  
requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred.  
EventID: 0x0000272C Time Generated: 06/19/2025 04:14:19 Event String: DCOM was unable  
to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any  
of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).  
An error event occurred. EventID: 0x0000272C Time Generated: 06/19/2025 04:14:19 Event  
String: DCOM was unable to communicate with the computer  
zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols;  
requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred.  
EventID: 0x0000272C Time Generated: 06/19/2025 04:23:02 Event String: DCOM was unable  
to communicate with the computer 192.168.0.1 using any of the configured protocols; requested  
by PID e04 (C:\Windows\system32\dcdiag.exe). An error event occurred. EventID: 0x0000272C  
Time Generated: 06/19/2025 04:23:23 Event String: DCOM was unable to communicate with  
the computer 1.1.1.1 using any of the configured protocols; requested by PID e04

(C:\Windows\system32\dcdiag.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/19/2025 04:23:44 Event String: DCOM was unable to communicate with the computer 9.9.9.9 using any of the configured protocols; requested by PID e04

(C:\Windows\system32\dcdiag.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/19/2025 04:24:02 Event String: DCOM was unable to communicate with the computer 192.168.0.1 using any of the configured protocols; requested by PID 13fc

(C:\Windows\system32\dcdiag.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/19/2025 04:24:19 Event String: DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/19/2025 04:24:19 Event String: DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/19/2025 04:24:19 Event String: DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/19/2025 04:24:19 Event String: DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/19/2025 04:24:23 Event String: DCOM was unable to communicate with the computer 1.1.1.1 using any of the configured protocols; requested by PID 13fc (C:\Windows\system32\dcdiag.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/19/2025 04:24:44 Event String: DCOM was unable to communicate with the computer 9.9.9.9 using any of the configured protocols; requested by PID 13fc

(C:\Windows\system32\dcdiag.exe). ..... WIN2016DC2 failed test SystemLog Starting test: Topology \* Configuration Topology Integrity Check \* Analyzing the connection topology for DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing upstream (of target) analysis. \* Performing downstream (of target) analysis. \* Analyzing the connection topology for DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing upstream (of target) analysis. \* Performing downstream (of target) analysis. \* Analyzing the connection topology for CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing upstream (of target) analysis. \* Performing downstream (of target) analysis. \* Analyzing the connection topology for CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing upstream (of target) analysis. \* Performing downstream (of target) analysis. \* Analyzing the connection topology for DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing upstream (of target) analysis. \* Performing downstream (of target) analysis. ....

WIN2016DC2 passed test Topology Starting test: VerifyEnterpriseReferences ..... WIN2016DC2 passed test VerifyEnterpriseReferences Starting test:

VerifyReferences The system object reference (serverReference)  
CN=WIN2016DC2,OU=Domain  
Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com and backlink on  
CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=H  
omeLab,DC=TechSavvyProductions,DC=com are correct. The system object  
reference (serverReferenceBL) CN=WIN2016DC2,CN=Topology,CN=Domain System  
Volume,CN=DFSR-GlobalSettings,CN=System,DC=HomeLab,DC=TechSavvyProducti  
ons,DC=com and backlink on CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,C

## STEP-BY-STEP TROUBLESHOOTING GUIDE FOR ALL ERRORS

---

### 1. Replication access was denied (Error 0x2105, Test: Replications & CheckSecurityError)

**Root Cause:** The current user or DC computer account lacks permission to query replication metadata — often caused by ACL corruption after manual DC removal.

#### **Fix:**

##### 1. Ensure your admin account is in these groups:

- o Domain Admins
- o Enterprise Admins
- o Administrators

##### 2. Take ownership of the NTDS Settings object:

- o Open adsiedit.msc
- o Connect to the **Configuration context**
- o Navigate to:

ini

CopyEdit

CN=NTDS

Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN  
=Configuration,...

- o Right-click → **Properties** → Security → Advanced
- o Change **Owner** to your account or Domain Admins
- o Then assign **Full Control**

### 3. Restart NTDS:

```
powershell  
CopyEdit  
net stop ntds  
net start ntds
```

### 4. Verify replication:

```
powershell  
CopyEdit  
repadmin /replsummary  
repadmin /showrepl
```

---

## 2. Test Services – Access Denied on NTDS

**Root Cause:** dcdiag run with insufficient privileges or permission corruption on NTDS service.

### Fix:

1. **Run PowerShell or CMD as Administrator**
2. Confirm NTDS service is running:

```
powershell  
CopyEdit  
Get-Service NTDS
```

If not:

```
powershell  
CopyEdit  
Start-Service NTDS
```

3. Check registry permissions:
  - o Run regedit
  - o Navigate to:

```
sql
```

CopyEdit

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS

- o Right-click → Permissions → Ensure SYSTEM and Administrators have full control

---

### 3. NetLogons Test – “User credentials does not have permission...”

**Root Cause:** Either your account lacks "Access this computer from the network" rights or SYSVOL/Netlogon shares are not authenticating correctly.

#### Fix:

##### 1. Run **secpol.msc**

- o Go to:

sql

CopyEdit

Local Policies → User Rights Assignment

- o Find:

- **Access this computer from the network**
- Ensure the following are present:
  - Administrators
  - Authenticated Users
  - Domain Admins

##### 2. Restart Netlogon:

powershell

CopyEdit

```
net stop netlogon
```

```
net start netlogon
```

##### 3. Force re-registration of SRV records:

powershell

CopyEdit

nltest /dsregdns

---

#### 4. DFS Replication Test – Event ID 0xC00004B2, Error 160

**Root Cause:** DFSR can't contact a now-dead domain controller (probably WIN2016DC3) or the config still references it.

##### **Fix:**

1. Open dfsmgmt.msc
  - o Expand **Replication** → SYSVOL
  - o Ensure only WIN2016DC2 is a member
  - o Remove any lingering connection/member pointing to WIN2016DC3
2. Manually trigger DFS config polling:

```
powershell
CopyEdit
dfsrdiag pollad
dfsrdiag backlog /rgname:"Domain System Volume" /partner:WIN2016DC2
/rfname:SYSVOL
```

3. If unresolved:
  - o Check:

```
ini
CopyEdit
CN=DFSR-LocalSettings,CN=WIN2016DC2,CN=Servers,...
```

in **ADSIEdit** and remove old connections.

---

#### 5. SystemLog Errors – DNS, DCOM, WinRM, Group Policy

These are mostly symptoms, not causes. Here's how to clean them up:

##### **DNS Registration Errors**

- Run:

```
powershell
CopyEdit
ipconfig /registerdns
nltest /dsregdns
```

- Restart DNS and Netlogon:

```
powershell
CopyEdit
net stop netlogon && net start netlogon
net stop dns && net start dns
```

### Group Policy Failures (Event ID 0x469)

- Make sure the network adapter has a valid IP, DNS points to 127.0.0.1 or local DC
- Force a group policy update:

```
powershell
CopyEdit
gpupdate /force
```

### DCOM/WinRM Errors

- Run:

```
cmd
CopyEdit
winrm quickconfig -q
netsh http add urlacl url=http://+:80/wsman/ user="NT
AUTHORITY\NETWORK SERVICE"
```

- Also reset SPNs:

```
cmd
CopyEdit
setspn -R win2016dc2
```

---

## ✓ AFTER FIXING: RETEST AD HEALTH

powershell

CopyEdit

```
dcdiag /v /c /e /f:"%userprofile%\Desktop\dcdiag_postfix.txt"
```

```
repadmin /replsummary
```

```
repadmin /showrepl
```

---

## ✓ Recommended: Schedule Cleanup and Reinforcement Tasks

Task	Command
Force DFSR Sync	dfsrdiag pollad
Reset Netlogon trust	netdom resetpwd /server:WIN2016DC2 /userd:administrator /passwordd:*
Check all FSMO roles	netdom query fsmo
Check DNS health	dcdiag /test:DNS
Schedule DNS scavenging	Use DNS Manager GUI

---

Would you like a PowerShell script or .ps1 utility to:

- Reset services
- Fix DFSR and Netlogon
- Re-register DNS
- Check FSMO and replication status

Let me know, and I'll build a cleanup-and-validate script for you.

**You said:**

build a cleanup-and-validate script

**ChatGPT said:**

Analyzed

python

Always show details

Copy

from textwrap import dedent

```
script_content = dedent("""
```

```
<#
```

```
.SYNOPSIS
```

```
    Post-Recovery AD Domain Controller Cleanup & Validation Script
```

```
.DESCRIPTION
```

```
    This script is designed for use after removing a failed domain controller.
```

```
    It repairs common issues such as Netlogon registration, DFSR errors, service restarts,
```

```
    DNS record re-registration, and validates FSMO roles and replication health.
```

```
.REQUIREMENTS
```

```
    - Run as Domain Admin on a healthy Domain Controller
```

```
    - PowerShell must be run as Administrator
```

```
#>
```

```
    Write-Host "Starting Domain Controller Cleanup and Validation..."
```

```
-ForegroundColor Cyan
```

```
# Section 1: Restart Critical Services
```

```
Write-Host "`n[1/6] Restarting Services..." -ForegroundColor Yellow
```

```
$services = "Netlogon", "DNS", "DFSR", "W32Time"
```

```
foreach ($svc in $services) {
```

```
    Write-Host "Restarting $svc..."
```

```
    Restart-Service -Name $svc -ErrorAction SilentlyContinue
```

```
}
```

```
# Section 2: Re-register DNS records
```

```
Write-Host "`n[2/6] Re-registering DNS Records..." -ForegroundColor Yellow
```

```
ipconfig /registerdns
```

```
nltest /dsregdns
```

```
# Section 3: Trigger DFSR Configuration Polling
```

```
Write-Host "`n[3/6] Polling DFSR AD Configuration..." -ForegroundColor Yellow
```

```
dfsrdiag pollad
```

```
# Section 4: Force Group Policy Update
```

```
Write-Host "`n[4/6] Forcing Group Policy Update..." -ForegroundColor Yellow  
gpupdate /force
```

```
# Section 5: Validate FSMO Roles
```

```
Write-Host "`n[5/6] FSMO Role Holders:" -ForegroundColor Yellow  
netdom query fsmo
```

```
# Section 6: Validate Replication and DCdiag Tests
```

```
Write-Host "`n[6/6] Validating Replication Health..." -ForegroundColor Yellow  
repadmin /replsummary  
repadmin /showrepl *
```

```
Write-Host "`nRunning DCdiag... This may take a few minutes..."  
-ForegroundColor Yellow  
dcdiag /v /c /e /f:"$env:USERPROFILE\Desktop\dcdiag_postfix.txt"
```

```
Write-Host "`nDone. See 'dcdiag_postfix.txt' on your Desktop for a full report."  
-ForegroundColor Green  
""")
```

```
# Save the script to a file
```

```
script_path = "/mnt/data/PostRecovery-ADCleanup.ps1"  
with open(script_path, "w") as f:  
    f.write(script_content)
```

```
script_path
```

```
Result
```

```
'/mnt/data/PostRecovery-ADCleanup.ps1'
```

 Your **Post-Recovery AD Cleanup & Validation PowerShell Script** is ready.

You can download it here:

 **PostRecovery-ADCleanup.ps1**

---

## What This Script Does:

1. **Restarts critical services:** Netlogon, DNS, DFSR, W32Time
2. **Re-registers DNS records** using ipconfig and nltest
3. **Polls DFSR AD configuration** to resolve SYSVOL sync issues
4. **Forces Group Policy update**
5. **Validates FSMO roles** with netdom query fsmo
6. **Checks replication health** via repadmin
7. **Runs full dcdiag** and saves output to your desktop as dcdiag\_postfix.txt

---

## Important Notes:

- Run this script **as Administrator** on WIN2016DC2
- Requires PowerShell 5.1 or newer
- Results are saved for follow-up review

Let me know if you'd like to extend this script to:

- Remove stale DNS records
- Auto-remove failed DC references in DFSR or AD Sites and Services
- Send the results via email or log to a file server

## You said:

build a cleanup-and-validate script

## ChatGPT said:

Here is a full-featured **PowerShell cleanup-and-validation script** specifically designed for a **post-domain controller recovery** scenario like yours. It restarts critical services, fixes DNS, validates replication, tests SYSVOL, and confirms FSMO roles.

---

## Features of the Script

- Restarts key services: Netlogon, DNS, W32Time, DFSR
  - Re-registers DNS records
  - Validates replication and NTDS health
  - Checks SYSVOL/Netlogon shares
  - Verifies FSMO role ownership
  - Saves a detailed dcdiag report to the desktop
- 

### **Script: PostRecovery-ADCleanup.ps1**

powershell

CopyEdit

<#

.SYNOPSIS

Post-Recovery Active Directory Cleanup and Validation Script

.DESCRIPTION

Designed for use after removing or losing a failed Domain Controller.

It resets services, repairs DNS and DFSR issues, and validates the remaining DC.

#>

Write-Host "Starting Domain Controller Post-Recovery Cleanup" -ForegroundColor Cyan

# Step 1: Restart essential services

\$services = "Netlogon", "DNS", "DFSR", "W32Time"

foreach (\$svc in \$services) {

Write-Host "Restarting \$svc..." -ForegroundColor Yellow

try {

Restart-Service -Name \$svc -ErrorAction Stop

} catch {

Write-Host "Failed to restart \$svc: \$\_" -ForegroundColor Red

}

}

# Step 2: Re-register DNS and SYSVOL

```
Write-Host "Re-registering DNS and restarting Netlogon for dynamic updates..."
-ForegroundColor Cyan
ipconfig /registerdns
nltest /dsregdns
Start-Sleep -Seconds 5
```

```
# Step 3: Force Group Policy update and DFSR poll
gpupdate /force
dfsrdiag pollad
```

```
# Step 4: Validate replication status
Write-Host "`nChecking replication summary..." -ForegroundColor Cyan
repadmin /replsummary
```


```
Write-Host "`nChecking individual replication partners..." -ForegroundColor Cyan
repadmin /showrepl *
```

```
# Step 5: FSMO Roles validation
Write-Host "`nFSMO Role Holders:" -ForegroundColor Cyan
netdom query fsmo
```

```
# Step 6: Check SYSVOL and NETLOGON shares
Write-Host "`nVerifying SYSVOL and NETLOGON shares..." -ForegroundColor Cyan
Test-Path "\\$env:COMPUTERNAME\SYSVOL | Out-Host
Test-Path "\\$env:COMPUTERNAME\NETLOGON | Out-Host
```

```
# Step 7: Run DCDIAG and save to Desktop
$dcdiagPath = "$env:USERPROFILE\Desktop\dcdiag_postfix.txt"
Write-Host "`nRunning full DCDIAG scan... Please wait." -ForegroundColor Yellow
dcdiag /v /c /e /f:$dcdiagPath
```

```
Write-Host "`nDCDIAG completed. Results saved to:" -ForegroundColor Green
Write-Host $dcdiagPath -ForegroundColor White
```

```
Write-Host "`n Active Directory cleanup script completed." -ForegroundColor Green
```

---

## How to Use

1. Save as: PostRecovery-ADCleanup.ps1
2. Right-click PowerShell → **Run as Administrator**
3. Execute the script:

```
powershell
CopyEdit
Set-ExecutionPolicy RemoteSigned -Scope Process
.\PostRecovery-ADCleanup.ps1
```

---

Would you like an advanced version that also:

- Checks for lingering objects
- Compares replication topology to expected state
- Emails results or writes to a central log share?

I can provide that too.

### **You said:**

```
PS E:\docs> .\PostRecovery-ADCleanup.ps1 At
E:\docs\PostRecovery-ADcleanup.ps1:19 char:39 + Write-Host "Failed to restart
$svc: $_" -ForegroundColor Red + ~~~~~ Variable reference is not valid. ':' was not
followed by a valid variable name character. Consider using ${} to delimit the
name. + CategoryInfo          : ParserError: (:) [], ParseException + FullyQualifiedErrorId :
InvalidVariableReferenceWithDrive
```

### **ChatGPT said:**

You're seeing the error because Write-Host is trying to display the error message using \$\_ **inside a double-quoted string**, but PowerShell expects variables inside "..." to be either simple (like \$svc) or wrapped in \${} if they are complex.

---

## Fix

Change this line:

```
powershell
CopyEdit
Write-Host "Failed to restart $svc: $_" -ForegroundColor Red
```

To this corrected version:

```
powershell
CopyEdit
Write-Host "Failed to restart $svc:`n$($_.Exception.Message)" -ForegroundColor
Red
```

This properly displays the name of the service and the actual exception message on a new line, which is cleaner and valid PowerShell.

---

### Fixed Section of Script

Here is the corrected block:

```
powershell
CopyEdit
foreach ($svc in $services) {
    Write-Host "Restarting $svc..." -ForegroundColor Yellow
    try {
        Restart-Service -Name $svc -ErrorAction Stop
    } catch {
        Write-Host "Failed to restart $svc:`n$($_.Exception.Message)"
-ForegroundColor Red
    }
}
```

---

Would you like the entire updated script re-posted or saved as a download file again?

**You said:**

```
.\PostRecovery-ADCleanup.ps1 At E:\docs\PostRecovery-ADCleanup.ps1:19
char:39 + Write-Host "Failed to restart $svc:n${($_.Exception.Message)" ... + ~~~~~
Variable reference is not valid. ':' was not followed by a valid variable name
character. Consider using ${} to delimit the name. + CategoryInfo          : ParserError: (:)
[], ParseException + FullyQualifiedErrorId : InvalidVariableReferenceWithDrive
```

### ChatGPT said:

Analysis errored

python

Always show details

Copy

from textwrap import dedent

```
# Correcting the script with proper variable referencing and re-saving
```

```
fixed_script = dedent("""
```

```
<#
```

```
.SYNOPSIS
```

```
    Post-Recovery AD Domain Controller Cleanup & Validation Script
```

```
.DESCRIPTION
```

```
    This script is designed for use after removing a failed domain controller.
```

```
    It repairs common issues such as Netlogon registration, DFSR errors, service
restarts,
```

```
    DNS record re-registration, and validates FSMO roles and replication health.
```

```
.REQUIREMENTS
```

```
    - Run as Domain Admin on a healthy Domain Controller
```

```
    - PowerShell must be run as Administrator
```

```
#>
```

```
    Write-Host "Starting Domain Controller Cleanup and Validation..."
```

```
-ForegroundColor Cyan
```

```
# Section 1: Restart Critical Services
```

```
Write-Host "`n[1/6] Restarting Services..." -ForegroundColor Yellow
```

```
$services = "Netlogon", "DNS", "DFSR", "W32Time"
```

```
foreach ($svc in $services) {
```

```
Write-Host "Restarting $svc..."
try {
    Restart-Service -Name $svc -ErrorAction Stop
} catch {
    Write-Host ("Failed to restart {0}: `n{1}" -f $svc, $_.Exception.Message)
-ForegroundColor Red
}
}
```

# Section 2: Re-register DNS records

```
Write-Host "`n[2/6] Re-registering DNS Records..." -ForegroundColor Yellow
ipconfig /registerdns
nltest /dsregdns
```

# Section 3: Trigger DFSR Configuration Polling

```
Write-Host "`n[3/6] Polling DFSR AD Configuration..." -ForegroundColor Yellow
dfsrdiag pollad
```

# Section 4: Force Group Policy Update

```
Write-Host "`n[4/6] Forcing Group Policy Update..." -ForegroundColor Yellow
gpupdate /force
```

# Section 5: Validate FSMO Roles

```
Write-Host "`n[5/6] FSMO Role Holders:" -ForegroundColor Yellow
netdom query fsmo
```

# Section 6: Validate Replication and DCdiag Tests

```
Write-Host "`n[6/6] Validating Replication Health..." -ForegroundColor Yellow
repadmin /replsummary
repadmin /showrepl *
```

```
Write-Host "`nRunning DCdiag... This may take a few minutes..."
-ForegroundColor Yellow
dcdiag /v /c /e /f:"$env:USERPROFILE\Desktop\dcdiag_postfix.txt"
```

```
Write-Host "`nDone. See 'dcdiag_postfix.txt' on your Desktop for a full report."
-ForegroundColor Green
```

```
""")
```

```
# Save corrected script
```

```
corrected_script_path = "/mnt/data/PostRecovery-ADCleanup_FIXED.ps1"
```

```
with open(corrected_script_path, "w") as f:
```

```
    f.write(fixed_script)
```

```
corrected_script_path
```

```
Analyzed
```

```
python
```

```
Always show details
```

```
Copy
```

```
from textwrap import dedent
```

```
# Re-define and save the corrected PowerShell script after kernel reset
```

```
fixed_script = dedent("""
```

```
<#
```

```
.SYNOPSIS
```

```
    Post-Recovery AD Domain Controller Cleanup & Validation Script
```

```
.DESCRIPTION
```

```
    This script is designed for use after removing a failed domain controller.
```

```
    It repairs common issues such as Netlogon registration, DFSR errors, service restarts,
```

```
    DNS record re-registration, and validates FSMO roles and replication health.
```

```
.REQUIREMENTS
```

```
    - Run as Domain Admin on a healthy Domain Controller
```

```
    - PowerShell must be run as Administrator
```

```
#>
```

```
    Write-Host "Starting Domain Controller Cleanup and Validation..."
```

```
-ForegroundColor Cyan
```

```
# Section 1: Restart Critical Services
```

```
Write-Host "`n[1/6] Restarting Services..." -ForegroundColor Yellow
```

```
$services = "Netlogon", "DNS", "DFSR", "W32Time"
```

```
foreach ($svc in $services) {
    Write-Host "Restarting $svc..."
    try {
        Restart-Service -Name $svc -ErrorAction Stop
    } catch {
        Write-Host ("Failed to restart {0}: `n{1}" -f $svc, $_.Exception.Message)
-ForegroundColor Red
    }
}

# Section 2: Re-register DNS records
Write-Host "`n[2/6] Re-registering DNS Records..." -ForegroundColor Yellow
ipconfig /registerdns
nltest /dsregdns

# Section 3: Trigger DFSR Configuration Polling
Write-Host "`n[3/6] Polling DFSR AD Configuration..." -ForegroundColor Yellow
dfsrdiag pollad

# Section 4: Force Group Policy Update
Write-Host "`n[4/6] Forcing Group Policy Update..." -ForegroundColor Yellow
gpupdate /force

# Section 5: Validate FSMO Roles
Write-Host "`n[5/6] FSMO Role Holders:" -ForegroundColor Yellow
netdom query fsmo

# Section 6: Validate Replication and DCdiag Tests
Write-Host "`n[6/6] Validating Replication Health..." -ForegroundColor Yellow
repadmin /replsummary
repadmin /showrepl *

Write-Host "`nRunning DCdiag... This may take a few minutes..."
-ForegroundColor Yellow
dcdiag /v /c /e /f:"$env:USERPROFILE\Desktop\dcdiag_postfix.txt"
```

```
Write-Host "`nDone. See 'dcdiag_postfix.txt' on your Desktop for a full report."
-ForegroundColor Green
""")
```

```
# Save corrected script
corrected_script_path = "/mnt/data/PostRecovery-ADCleanup_FIXED.ps1"
with open(corrected_script_path, "w") as f:
    f.write(fixed_script)
```

```
corrected_script_path
Result
'/mnt/data/PostRecovery-ADCleanup_FIXED.ps1'
```

 The corrected PowerShell script is ready for download:

 **Download PostRecovery-ADCleanup\_FIXED.ps1**

This version fixes the `$_` variable formatting issue and is safe to run using PowerShell with administrator rights.

Let me know if you want an extended version with email logging or lingering object cleanup!

### You said:

```
At E:\docs\PostRecovery-ADcleanup.ps1:1 char:1 + from textwrap import dedent
+ ~~~~ The 'from' keyword is not supported in this version of the language. At
E:\docs\PostRecovery-ADcleanup.ps1:19 char:17 + Write-Host "Starting Domain
Controller Cleanup and Validation..." ... + ~~~~~~ Unexpected token 'Starting' in
expression or statement. At E:\docs\PostRecovery-ADcleanup.ps1:19 char:17 +
Write-Host "Starting Domain Controller Cleanup and Validation..." ... + ~ Missing
closing ')' in expression. At E:\docs\PostRecovery-ADcleanup.ps1:59 char:4 + """) +
~ Unexpected token ')' in expression or statement. At
E:\docs\PostRecovery-ADcleanup.ps1:63 char:32 + with
open(corrected_script_path, "w") as f: + ~ Missing argument in parameter list. +
CategoryInfo          : ParserError: (:) [], ParseException + FullyQualifiedErrorId :
ReservedKeywordNotAllowed
```

### ChatGPT said:

The errors you're seeing are due to attempting to **run a Python script inside PowerShell**. The content you posted includes Python syntax like from textwrap import dedent and with open(...), which **is not valid in PowerShell**.

---

### **What Went Wrong**

You accidentally copied Python code (used internally here to generate a PowerShell script) into your PowerShell environment. Instead, you should **only copy the actual PowerShell script content**, not the script that generated it.

---

### **How to Fix It**

Download and run the corrected **PowerShell script file** that I've already prepared for you:

 **[Click here to download the correct script](#)**

Then follow these steps:

---

### **Instructions to Use the Script**

1. **Move the .ps1 file to your domain controller** (e.g., E:\docs\)
2. Open **PowerShell as Administrator**
3. Run:

```
powershell
CopyEdit
Set-ExecutionPolicy RemoteSigned -Scope Process
E:\docs\PostRecovery-ADCleanup_FIXED.ps1
```

---

Would you like a version of the script that logs all actions to a .log file as well as the screen?

## You said:

Set-ExecutionPolicy : Windows PowerShell updated your execution policy successfully, but the setting is overridden by a policy defined at a more specific scope. Due to the override, your shell will retain its current effective execution policy of RemoteSigned. Type "Get-ExecutionPolicy -List" to view your execution policy settings. For more information please see "Get-Help Set-ExecutionPolicy".  
At line:1 char:1 + Set-ExecutionPolicy -executionPolicy Unrestricted +  
~~~~~ + CategoryInfo :  
PermissionDenied: (:) [Set-ExecutionPolicy], SecurityException +  
FullyQualifiedErrorId :  
ExecutionPolicyOverride,Microsoft.PowerShell.Commands.SetExecutionPolicyCommand

## ChatGPT said:

You're encountering the following message:

Set-ExecutionPolicy : ... the setting is overridden by a policy defined at a more specific scope.

This means there's a **Group Policy (GPO)** or **machine-wide configuration** enforcing the current PowerShell execution policy, preventing changes even with administrator rights.

---

### ✔ Solution Options

#### ✔ Option 1: Use Bypass for This Session Only

You can run the script without changing the global policy by using the -ExecutionPolicy Bypass flag:

```
powershell  
CopyEdit  
powershell.exe -ExecutionPolicy Bypass -File  
"E:\\docs\\PostRecovery-ADCleanup_FIXED.ps1"
```

✓ This temporarily bypasses execution policy **just for this session** — it's the safest and quickest workaround.

---

## 🔍 Option 2: Check What's Enforcing the Policy

To investigate what's locking the policy:

```
powershell  
CopyEdit  
Get-ExecutionPolicy -List
```

Output will look like:

```
mathematica  
CopyEdit  
  Scope ExecutionPolicy  
  -----  
MachinePolicy  Undefined  
  UserPolicy   Undefined  
  Process      Undefined  
  CurrentUser  RemoteSigned  
LocalMachine   RemoteSigned
```

If **MachinePolicy** or **UserPolicy** is set to AllSigned or Restricted, it is being enforced by **Group Policy**.

To lift that:

- Open Group Policy Editor: gpedit.msc
- Navigate to:

```
nginx  
CopyEdit  
Computer Configuration > Administrative Templates > Windows  
Components > Windows PowerShell
```


- Set "**Turn on Script Execution**" to:

css  
CopyEdit  
Enabled > Allow all scripts

Then run:

powershell  
CopyEdit  
gpupdate /force

---

 **Recommended: Use Option 1 to Run the Script Immediately**

powershell  
CopyEdit  
powershell.exe -ExecutionPolicy Bypass -File  
"E:\\docs\\PostRecovery-ADCleanup\_FIXED.ps1"

Let me know if you'd like a version of the script that:

- Writes all output to a .log file
- Sends summary email to an admin
- Automatically detects and lists remaining metadata related to the removed DC

**You said:**

PostRecovery-ADCleanup.ps1  
9  
1  
2  
powershell.exe -ExecutionPolicy Bypass -File  
"E:\\docs\\PostRecovery-ADCleanup.ps1"

**ChatGPT said:**

Great — I see you've created a launcher line to run your script with execution policy bypass. If you'd like, I can help expand this file into a full **Post-Recovery Cleanup and Validation Script** inside your canvas document.

Would you like me to:

1. **Replace** the single line with the complete PowerShell script content?
2. **Add logging** to output results to a .log file?
3. **Keep the execution line and just append the script** underneath?

Let me know how you'd like to proceed.

**You said:**

```
PS E:\docs> Set-ExecutionPolicy -executionPolicy Unrestricted Execution Policy
Change The execution policy helps protect you from scripts that you do not trust.
Changing the execution policy might expose you to the security risks described in
the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the
execution policy? [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "N"): a Set-ExecutionPolicy : Windows PowerShell updated your
execution policy successfully, but the setting is overridden by a policy defined at a
more specific scope. Due to the override, your shell will retain its current effective
execution policy of RemoteSigned. Type "Get-ExecutionPolicy -List" to view your
execution policy settings. For more information please see "Get-Help
Set-ExecutionPolicy". At line:1 char:1 + Set-ExecutionPolicy -executionPolicy
Unrestricted + ~~~~~ +
CategoryInfo          : PermissionDenied: (:) [Set-ExecutionPolicy], SecurityException +
FullyQualifiedErrorId :
ExecutionPolicyOverride,Microsoft.PowerShell.Commands.SetExecutionPolicyCom
mand PS E:\docs> powershell.exe -ExecutionPolicy Bypass -File
"E:\docs\PostRecovery-ADCleanup.ps1" File
E:\docs\PostRecovery-ADCleanup.ps1 cannot be loaded. The file
E:\docs\PostRecovery-ADCleanup.ps1 is not digitally signed. You cannot run this
script on the current system. For more information about running scripts and
setting execution policy, see about_Execution_Policies at
http://go.microsoft.com/fwlink/?LinkID=135170. + CategoryInfo          : SecurityError: (:)

```

[], ParentContainsErrorRecordException + FullyQualifiedErrorId : UnauthorizedAccess

### ChatGPT said:

You're facing two **overlapping execution policy enforcement issues**:

---

#### What's Happening:

1. **Your PowerShell environment is locked down by Group Policy**, so even if you try Set-ExecutionPolicy, it's overridden.
2. **Your system enforces a "signed scripts only" policy**, meaning **unsigned scripts** (like the .ps1 you're trying to run) are **blocked**.

This behavior is typical in:

- **Domain-joined systems**
  - **Servers with security baselines**
  - **Environments with GPOs enforcing AllSigned or RemoteSigned globally**
- 

#### Solution: Use Inline Execution to Bypass the Policy

You can **execute the contents of the script inline** instead of calling the file directly.

#### Step 1: Copy the contents of PostRecovery-ADCleanup.ps1

Paste it into a new elevated PowerShell window **manually** OR...

#### Step 2: Use Invoke-Command to run the script inline:

```
powershell
CopyEdit
Invoke-Command -ScriptBlock {
    # Restart critical services
    $services = "Netlogon", "DNS", "DFSR", "W32Time"
    foreach ($svc in $services) {
```

```

Write-Host "Restarting $svc..."
try {
    Restart-Service -Name $svc -ErrorAction Stop
} catch {
    Write-Host ("Failed to restart {0}: `n{1}" -f $svc, $_.Exception.Message)
-ForegroundColor Red
}
}

# DNS re-registration
ipconfig /registerdns
nltest /dsregdns

# Force policy and DFSR update
gpupdate /force
dfsrdiag pollad

# Replication and FSMO checks
repadmin /replsummary
repadmin /showrepl *
netdom query fsmo

# Check SYSVOL and Netlogon shares
Test-Path "\\$env:COMPUTERNAME\SYSVOL | Out-Host
Test-Path "\\$env:COMPUTERNAME\NETLOGON | Out-Host

# DCDiag output to Desktop
dcdiag /v /c /e /f:"$env:USERPROFILE\Desktop\dcdiag_postfix.txt"
}

```

This avoids script file execution and **bypasses signing enforcement**.

---

### **Optional: Digitally Sign the Script (if needed)**

If you're in a secure domain, you may eventually want to:

1. **Create a Code Signing Certificate**
2. **Sign the script** using:

powershell

CopyEdit

```
Set-AuthenticodeSignature -FilePath "E:\\docs\\PostRecovery-ADCleanup.ps1"  
-Certificate (Get-ChildItem -Path Cert:\\CurrentUser\\My -CodeSigningCert)
```

But for now, the Invoke-Command inline block is your cleanest workaround.

---

Would you like me to insert the **inline version of the script directly into your canvas document** so you can run it as-is from PowerShell?

**You said:**

```
PS C:\Windows\system32> Invoke-Command -ScriptBlock { >> # Restart critical  
services >> $services = "Netlogon", "DNS", "DFSR", "W32Time" >> foreach ($svc in  
$services) { >> Write-Host "Restarting $svc..." >> try { >> Restart-Service -Name  
$svc -ErrorAction Stop >> } catch { >> Write-Host ("Failed to restart {0}: n{1}" -f  
$svc, $_.Exception.Message) -ForegroundColor Red >> } >> } >> # DNS  
re-registration >> ipconfig /registerdns >> nltest /dsregdns >> >> # Force policy  
and DFSR update >> gpupdate /force >> dfsrdiag pollad >> >> # Replication and  
FSMO checks >> repadmin /replsummary >> repadmin /showrepl * >> netdom  
query fsmo >> >> # Check SYSVOL and Netlogon shares >> Test-Path  
\\$env:COMPUTERNAME\SYSTEM\sysvol | Out-Host >> Test-Path  
\\$env:COMPUTERNAME\NETLOGON | Out-Host >> >> # DCdiag output to  
Desktop >> dcdiag /v /c /e /f:"$env:USERPROFILE\Desktop\dcdiag_postfix.txt"  
>> } Restarting Netlogon... WARNING: Waiting for service 'Netlogon (Netlogon)' to  
start... Restarting DNS... Restarting DFSR... Restarting W32Time... Windows IP  
Configuration Registration of the DNS resource records for all adapters of this  
computer has been initiated. Any errors will be reported in the Event Viewer in 15  
minutes. Flags: 0 Connection Status = 0 0x0 NERR_Success The command  
completed successfully Updating policy... Computer Policy update has completed  
successfully. User Policy update has completed successfully. Operation Succeeded  
Replication Summary Start Time: 2025-06-19 09:37:47 Beginning data collection  
for replication summary, this may take awhile: .... Source DSA largest delta  
fails/total %% error Destination DSA largest delta fails/total %% error Repadmin:
```

```
running command /showrepl against full DC
Win2016DC2.HomeLab.TechSavvyProductions.com HQ-Homelab\WIN2016DC2
DSA Options: IS_GC Site Options: (none) DSA object GUID:
60228dba-cbc8-4304-868a-28f53a302f46 DSA invocationID:
7a35f1f8-1dce-4399-9264-25fdb678ef21 Schema master
Win2016DC2.HomeLab.TechSavvyProductions.com Domain naming master
Win2016DC2.HomeLab.TechSavvyProductions.com PDC
Win2016DC2.HomeLab.TechSavvyProductions.com RID pool manager
Win2016DC2.HomeLab.TechSavvyProductions.com Infrastructure master
Win2016DC2.HomeLab.TechSavvyProductions.com The command completed
successfully. True True PS C:\Windows\system32>
```

### ChatGPT said:

✔ **Success!** Your inline cleanup-and-validation PowerShell script **ran perfectly** and confirms:

---

### Summary of Results

#### ◆ Services Restarted:

- ✔ Netlogon
- ✔ DNS
- ✔ DFSR
- ✔ W32Time


#### ◆ DNS & SYSVOL

- ✔ DNS resource records re-registered
- ✔ \\WIN2016DC2\SYSVOL and \\WIN2016DC2\NETLOGON confirmed accessible (True, True)

#### ◆ Group Policy

- ✔ gpupdate completed successfully for both computer and user policy

#### ◆ DFS Replication Config

-  dfsrdiag pollad succeeded

#### ◆ **FSMO Role Holders**





All 5 FSMO roles are now held by:

Win2016DC2.HomeLab.TechSavvyProductions.com

#### ◆ **Replication Status**

- No current partners = expected if only 1 DC remains
  - No replication errors reported
- 

#### **Next Recommended Steps**

1.  **Open dcdiag\_postfix.txt** on your Desktop  
(This contains the full AD health check report)
  2.  If you plan to add a new DC:
    - Run: dcpromo or Install-ADDSDomainController
    - Allow SYSVOL and DFS replication to sync
  3.  Clean DNS:
    - Remove stale records for the failed win2016dc3
    - Use dnsmgmt.msc and clean up \_msdcs, \_sites, etc.
  4.  Optionally audit ACLs:
    - Especially on CN=NTDS Settings to ensure no orphaned permissions
- 

#### **Bonus Offer**

Would you like a follow-up script to:

-  Automatically clean **stale DNS and SRV records**
-  Check and remove **lingering objects**
-  Email or log status reports to a file share or admin inbox?

Let me know how you want to enhance this further. You're nearly done recovering from the failed DC!

## You said:

Automatically clean stale DNS and SRV records

## ChatGPT said:

Clean Stale Dnsrecords

✅ The **PowerShell script to automatically clean stale DNS and SRV records** has been created in your canvas as CleanStaleDNSRecords.ps1.

---

## How to Use This Script

### ◆ Parameters Required:

- -DCName → The hostname of the decommissioned DC (e.g. WIN2016DC3)
- -DCIPv4 → The old IP address (e.g. 192.168.0.233)

### ◆ Example Command:

```
.\CleanStaleDNSRecords.ps1 -DCName "WIN2016DC3" -DCIPv4 "192.168.0.233"
```

---

## What It Does

| Record Type | Location                     | Action                            |
|-------------|------------------------------|-----------------------------------|
| A           | Forward zones                | Matches DCName and DCIPv4         |
| PTR         | Reverse lookup zones         | Matches pointer records to DCName |
| SRV         | _msdcs, _sites, domain zones | Matches service records to DCName |

All matched records are removed with -Force silently if found.

---

Would you like to extend this to:

- Log changes to a .txt file?
- Support dry-run mode (show without deleting)?

- Email a summary of what was deleted?

Let me know and I'll expand it accordingly.

**You said:**

Automatically clean stale DNS and SRV records and Check and remove lingering objects using command-line

**ChatGPT said:**

Clean Stale Dnsrecords

99

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
<#

.SYNOPSIS

Automatically cleans stale A, PTR, and SRV DNS records and removes lingering objects from AD.

.DESCRIPTION

This script:

- Removes stale DNS A, PTR, and SRV records for a decommissioned Domain Controller.
- Detects and removes lingering objects using repadmin.

.PARAMETER DCName

The hostname of the decommissioned Domain Controller (e.g., "WIN2016DC3").

.PARAMETER DCIPv4

The IPv4 address of the decommissioned Domain Controller (e.g., "192.168.0.233").

#>

```
param(  
[Parameter(Mandatory)]  
[string]$DCName,  
  
[Parameter(Mandatory)]  
[string]$DCIPv4
```

)

```
Write-Host "Starting DNS and Lingering Object cleanup for: $DCName ($DCIPv4)"  
-ForegroundColor Cyan
```

```
Import-Module DNSServer -ErrorAction Stop
```


```
# Step 1: Remove A record from Forward Lookup Zone  
$zone = (Get-DnsServerZone | Where-Object { $_.ZoneType -eq 'Primary' -and  
$_ .IsReverseLookupZone -eq $false })  
foreach ($z in $zone) {  
try {  
$records = Get-DnsServerResourceRecord -ZoneName $z.ZoneName -Name  
$DCName -ErrorAction Stop  
foreach ($record in $records) {  
if ($record.RecordType -eq 'A' -and  
$record.RecordData.IPv4Address.IPAddressToString -eq $DCIPv4) {  
Edited Clean Stale Dnsrecords
```

 The script now automatically:

1. **Removes stale DNS records** (A, PTR, SRV) for a decommissioned domain controller
2. **Checks and removes lingering AD objects** using repadmin

You can run the updated script like this:

```
powershell  
CopyEdit  
.\CleanStaleDNSRecords.ps1 -DCName "WIN2016DC3" -DCIPv4 "192.168.0.233"
```

 **Tip:** The lingering object cleanup includes an /advisory\_mode pass first, so you can verify what would be removed before actual deletion.

Would you like to include:

- A logging option to save actions to a .log file?
- A dry-run mode that only shows what would be deleted?

Let me know, and I'll add those features.

**You said:**

is this python?

**ChatGPT said:**

No — the script in your canvas is **not Python**. It is written in **PowerShell**, a command-line scripting language used for automating tasks in Windows environments.

### **How You Know It's PowerShell:**

- It uses **param()** blocks for parameter handling
- Cmdlets like:
  - Get-DnsServerZone
  - Remove-DnsServerResourceRecord
  - Write-Host
- It interacts with Windows DNS, Active Directory, and repadmin

### **What This Script Does:**

- Removes stale **A**, **PTR**, and **SRV** records in DNS
- Cleans **lingering AD objects** using repadmin
- Uses Get-ADDomain, Get-ADDomainController to dynamically pull directory info
- Designed for **Domain Controller cleanup automation**

---

Would you like a side-by-side comparison with a Python version for educational purposes, or are you planning to run this on a specific Windows Server host?

**You said:**

I am slowly cleaning AD's meta data on my remainin, I lost win2016dc3 which was on a VM hosted by a NVMe. I can not remove some data from AD sites and services even though I have membership with Enterprise Admin. DNS has been cleaned of the failed domain controller win2016dc2, below is the results of Win2016dc2's dcdiag. Directory Server Diagnosis Performing initial setup: Trying to find home server... \* Verifying that the local machine

Win2016DC2, is a Directory Server. Home Server = Win2016DC2 \* Connecting to directory service on server Win2016DC2. \* Identified AD Forest. Collecting AD specific global data \* Collecting site info. Calling ldap\_search\_init\_page(hld,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com,LDAP\_SCOPE\_SUBTREE,(objectCategory=ntDSsiteSettings),..... The previous call succeeded Iterating through the sites Looking at base site object: CN=NTDS Site Settings,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com Getting ISTG and options for the site Looking at base site object: CN=NTDS Site Settings,CN=Mikrotek,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com Getting ISTG and options for the site \* Identifying all servers. Calling ldap\_search\_init\_page(hld,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com,LDAP\_SCOPE\_SUBTREE,(objectClass=ntDSDsa),..... The previous call succeeded.... The previous call succeeded Iterating through the list of servers Getting information for the server CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com objectGuid obtained InvocationID obtained dnsHostname obtained site info obtained All the info for the server collected \* Identifying all NC cross-refs. \* Found 1 DC(s). Testing 1 of them. Done gathering initial info. Doing initial required tests Testing server: HQ-Homelab\WIN2016DC2 Starting test: Connectivity \* Active Directory LDAP Services Check Determining IP4 connectivity \* Active Directory RPC Services Check ..... WIN2016DC2 passed test Connectivity Doing primary tests Testing server: HQ-Homelab\WIN2016DC2 Starting test: Advertising The DC WIN2016DC2 is advertising itself as a DC and having a DS. The DC WIN2016DC2 is advertising as an LDAP server The DC WIN2016DC2 is advertising as having a writable directory The DC WIN2016DC2 is advertising as a Key Distribution Center The DC WIN2016DC2 is advertising as a time server The DS WIN2016DC2 is advertising as a GC. .... WIN2016DC2 passed test Advertising Starting test: CheckSecurityError \* Dr Auth: Beginning security errors check! Found KDC WIN2016DC2 for domain HomeLab.TechSavvyProductions.com in site HQ-Homelab Checking machine account for DC WIN2016DC2 on DC WIN2016DC2. \* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com \* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com \* SPN found :LDAP/WIN2016DC2 \* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB \* SPN found :LDAP/60228dba-cbc8-4304-868a-28f53a302f46.\_msdcs.HomeLab.TechSavvyProductions.com \* SPN found :E3514235-4B06-11D1-AB04-00C04FC2DCD2/60228dba-cbc8-4304-868a-28f53a302f46/HomeLab.TechSavvyProductions.com \* SPN found :HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com \* SPN found :HOST/Win2016DC2.HomeLab.TechSavvyProductions.com \* SPN found :HOST/WIN2016DC2 \* SPN found :HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB \* SPN found :GC/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com [WIN2016DC2] DsReplicaGetInfo(KCC\_DS\_CONNECT\_FAILURES) failed with error 8453, Replication access was denied.. [WIN2016DC2] Unable to query the list of KCC connection failures. Continuing... [WIN2016DC2] No security related replication errors were found on this

DC! To target the connection to a specific source DC use /ReplSource:<DC>. ....

WIN2016DC2 passed test CheckSecurityError Starting test: CutoffServers \* Configuration Topology Aliveness Check \* Analyzing the alive system replication topology for DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing upstream (of target) analysis. \* Performing downstream (of target) analysis. \* Analyzing the alive system replication topology for DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing upstream (of target) analysis. \* Performing downstream (of target) analysis. \* Analyzing the alive system replication topology for CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing upstream (of target) analysis. \* Performing downstream (of target) analysis. \* Analyzing the alive system replication topology for CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing upstream (of target) analysis. \* Performing downstream (of target) analysis. \* Analyzing the alive system replication topology for DC=HomeLab,DC=TechSavvyProductions,DC=com. \* Performing upstream (of target) analysis. \* Performing downstream (of target) analysis. ....

WIN2016DC2 passed test CutoffServers Starting test: FrsEvent \* The File Replication Service Event log test Skip the test because the server is running DFSR. .... WIN2016DC2 passed test FrsEvent Starting test: DFSREvent The DFS Replication Event Log. ....

WIN2016DC2 passed test DFSREvent Starting test: SysVolCheck \* The File Replication Service SYSVOL ready test File Replication Service's SYSVOL is ready .... WIN2016DC2 passed test SysVolCheck Starting test: FrsSysVol \* The File Replication Service SYSVOL ready test File Replication Service's SYSVOL is ready .... WIN2016DC2 passed test FrsSysVol Starting test: KccEvent \* The KCC Event log test Found no KCC errors in "Directory Service" Event log in the last 15 minutes. .... WIN2016DC2 passed test KccEvent Starting test: KnowsOfRoleHolders Role Schema Owner = CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com Role Domain Owner = CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com Role PDC Owner = CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com Role Rid Owner = CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com Role Infrastructure Update Owner = CN=NTDS Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com .... WIN2016DC2 passed test KnowsOfRoleHolders Starting test: MachineAccount Checking machine account for DC WIN2016DC2 on DC WIN2016DC2. \* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com \* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com \* SPN found :LDAP/WIN2016DC2 \* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB \* SPN found :LDAP/60228dba-cbc8-4304-868a-28f53a302f46.\_msdcs.HomeLab.TechSavvyProductions.com \* SPN found :E3514235-4B06-11D1-AB04-00C04FC2DCD2/60228dba-cbc8-4304-868a-28f53a302f46/HomeLab.TechSavvyProductions.com \* SPN found

:HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com \* SPN found :HOST/Win2016DC2.HomeLab.TechSavvyProductions.com \* SPN found  
:HOST/WIN2016DC2 \* SPN found  
:HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB \* SPN found  
:GC/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com  
..... WIN2016DC2 passed test MachineAccount Starting test: NCSecDesc \* Security  
Permissions check for all NC's on DC WIN2016DC2. \* Security Permissions Check for  
DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com (NDNC,Version 3) \*  
Security Permissions Check for  
DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com (NDNC,Version 3)  
\* Security Permissions Check for  
CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(Schema,Version 3) \* Security Permissions Check for  
CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com (Configuration,Version  
3) \* Security Permissions Check for DC=HomeLab,DC=TechSavvyProductions,DC=com  
(Domain,Version 3) ..... WIN2016DC2 passed test NCSecDesc Starting test:  
NetLogons \* Network Logons Privileges Check Verified share \\WIN2016DC2\netlogon  
Verified share \\WIN2016DC2\sysvol [WIN2016DC2] User credentials does not have  
permission to perform this operation. The account used for this test must have network logon  
privileges for this machine's domain. .... WIN2016DC2 failed test NetLogons  
Starting test: ObjectsReplicated WIN2016DC2 is in domain  
DC=HomeLab,DC=TechSavvyProductions,DC=com Checking for  
CN=WIN2016DC2,OU=Domain  
Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com in domain  
DC=HomeLab,DC=TechSavvyProductions,DC=com on 1 servers Object is up-to-date on all  
servers. Checking for CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=  
HomeLab,DC=TechSavvyProductions,DC=com in domain  
CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com on 1 servers Object is  
up-to-date on all servers. .... WIN2016DC2 passed test ObjectsReplicated Starting  
test: OutboundSecureChannels \* The Outbound Secure Channels test \*\* Did not run Outbound  
Secure Channels test because /testdomain: was not entered ..... WIN2016DC2  
passed test OutboundSecureChannels Starting test: Replications \* Replications Check  
[Replications Check,WIN2016DC2] DsReplicaGetInfo(PENDING\_OPS, NULL) failed, error  
0x2105 "Replication access was denied." ..... WIN2016DC2 failed test Replications  
Starting test: RidManager \* Available RID Pool for the Domain is 14600 to 1073741823 \*  
Win2016DC2.HomeLab.TechSavvyProductions.com is the RID Master \* DsBind with RID  
Master was successful \* rIDAllocationPool is 4100 to 4599 \* rIDPreviousAllocationPool is 4100  
to 4599 \* rIDNextRID: 4101 ..... WIN2016DC2 passed test RidManager Starting  
test: Services \* Checking Service: EventSystem \* Checking Service: RpcSs \* Checking Service:  
NTDS Could not open NTDS Service on WIN2016DC2, error 0x5 "Access is denied." \*  
Checking Service: DnsCache \* Checking Service: DFSR \* Checking Service: IsmServ \*  
Checking Service: kdc \* Checking Service: SamSs \* Checking Service: LanmanServer \*  
Checking Service: LanmanWorkstation \* Checking Service: w32time \* Checking Service:  
NETLOGON ..... WIN2016DC2 failed test Services Starting test: SystemLog \* The  
System Event log test An error event occurred. EventID: 0x0000272C Time Generated:



to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/21/2025 08:44:18 Event String: DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/21/2025 08:44:18 Event String: DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/21/2025 08:54:18 Event String: DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/21/2025 08:54:18 Event String: DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/21/2025 08:54:18 Event String: DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/21/2025 09:04:18 Event String: DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/21/2025 09:04:18 Event String: DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe). An error event occurred. EventID: 0x0000272C Time Generated: 06/21/2025 09:04:18 Event String: DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

ChatGPT said:

Thanks for the detailed `dcdiag` output — it's clear you're doing a methodical post-mortem cleanup after the failure of `WIN2016DC3`. Here's a structured plan to **remove the leftover metadata, forcefully clean lingering objects**, and **validate** that `WIN2016DC3` is completely purged from Active Directory.

---

## Step-by-Step Cleanup Plan for WIN2016DC3

### 1. Seize FSMO Roles (already done?)

You've already confirmed WIN2016DC2 owns **all FSMO roles**, so this step is complete:

```
netdom query fsmo
```

If needed:

```
ntdsutil  
roles  
connections  
connect to server WIN2016DC2  
quit  
seize <role>
```

---

## 2. Forceful Metadata Cleanup of WIN2016DC3

### Option A: PowerShell (preferred on Win2016+)

```
Remove-ADObject -Identity "CN=NTDS  
Settings,CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configurati  
on,DC=HomeLab,DC=TechSavvyProductions,DC=com" -Recursive -Confirm:$false
```

### Then clean the Server object:

```
Remove-ADObject -Identity  
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=  
HomeLab,DC=TechSavvyProductions,DC=com" -Recursive -Confirm:$false
```

If you get **access denied**, ensure:

- You're **running as Enterprise Admin**
- Your DC isn't in **Safe Mode Read-Only mode**
- Use **"Run as Administrator"** PowerShell

## Option B: ntdsutil Interactive Method

```
ntdsutil
metadata cleanup
connections
connect to server WIN2016DC2
quit
select operation target
list sites
select site <number>
list servers in site
select server <number>
quit
remove selected server
```

---

## 3. Remove Lingering Objects from WIN2016DC2

Advisory (non-destructive):

```
repadmin /removelingerobjects WIN2016DC2 <GUID of
WIN2016DC2> /advisory_mode
```

Then destructive:

```
repadmin /removelingerobjects WIN2016DC2 <GUID of WIN2016DC2>
```

You can retrieve the DC GUID using:

```
Get-ADDomainController -Identity WIN2016DC2 | Select-Object Name,
ObjectGUID
```

---

## 4. Verify and Cleanup from AD Sites and Services GUI

Sometimes GUI stubbornness is due to background replication delays.

Try from another DC (if available) or use **adsiedit.msc**:

- Navigate to:  
Configuration -> Sites -> HQ-Homelab -> Servers
  - Delete:
    - CN=WIN2016DC3
    - Its NTDS Settings child
  - Also check:  
CN=Deleted Objects,...
- 

## 5. DNS Cleanup (You've done this, just verifying)

Your earlier PowerShell script took care of this, but double-check:

- Forward zones: WIN2016DC3
  - `_msdcs` and `SRV _ldap, _kerberos, _gc`
  - Reverse lookup zones: matching PTRs
- 

## 6. Re-run Validation

**Check for server remnants:**

```
Get-ADObject -Filter 'Name -like "*WIN2016DC3*"'  
-IncludeDeletedObjects -Properties *
```

**Verify replication health:**

```
repadmin /replsummary  
repadmin /showrepl *
```

**Final dcdiag:**

```
dcdiag /v /c /e  
/f: "$env:USERPROFILE\Desktop\postcleanup_dcdiag.txt"
```

---

## ⚠ Noteworthy Errors in Your dcdiag

- Replication access was denied: Often due to missing permissions or service issues. Clean lingering metadata.
- NTDS service access denied: Could point to corrupted service account or security descriptor. Removing orphaned server should help.
- NetLogons test failed: Expected if the machine account for WIN2016DC2 had permissions issues. Try resetting the secure channel:

Test-ComputerSecureChannel -Repair -Verbose

---

## Optional Cleanup Script

Would you like a single PowerShell script to:

- Delete all CN=WIN2016DC3 traces
- Remove lingering objects
- Recheck replication
- Validate cleanup

I can build this into a new canvas or integrate it into your current PowerShell cleanup suite.

Would you prefer it interactive or fully automated?

### You said:

```
Remove-ADObject -Identity "CN=NTDS
Settings,CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Con
figuration,DC=HomeLab,DC=TechSavvyProductions,DC=com" -Recursive
-Confirm:$false Remove-ADObject : Directory object not found At line:1 char:1 +
Remove-ADObject -Identity "CN=NTDS Settings,CN=WIN2016DC3,CN=Servers, ... +
~~~~~
~~ + CategoryInfo          : ObjectNotFound: (CN=NTDS
Setting...ductions,DC=com:ADObject) [Remove-ADObject], ADIdenti
tyNotFoundException + FullyQualifiedErrorId :
ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityNotFou
```

ndException,M  
icrosoft.ActiveDirectory.Management.Commands.RemoveADObject

---

## ✓ Step-by-Step Follow-Up

### 1. 🔍 Check what still exists

Try this PowerShell to list all objects that still reference WIN2016DC3:

```
powershell  
CopyEdit  
Get-ADObject -Filter 'Name -like "*WIN2016DC3*"' -Properties  
DistinguishedName | Format-List Name, DistinguishedName
```

#### Also try by CN=Servers path:

```
powershell  
CopyEdit  
Get-ADObject -LDAPFilter "(cn=WIN2016DC3)" -SearchBase  
"CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=Tech  
SavvyProductions,DC=com"
```

If anything is returned, grab the DistinguishedName and run:

```
powershell  
CopyEdit  
Remove-ADObject -Identity "<DistinguishedNameHere>" -Recursive  
-Confirm:$false
```

---

### 2. 🧠 Use ADSIEdit (for orphaned metadata)

If PowerShell fails but Sites and Services still shows ghost objects:

#### Steps:

1. Run adsiedit.msc
2. Connect to the **Configuration Naming Context**
3. Navigate to:

```
cpp
CopyEdit
CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com
  → CN=Sites
    → CN=HQ-Homelab
      → CN=Servers
        → CN=WIN2016DC3 ← delete this
```

4. Delete CN=WIN2016DC3 (and its child if still there: NTDS Settings)
  5. Refresh or close/reopen MMC to verify it's gone
- 

### 3. 🧹 Clean lingering objects

Run this from an **elevated CMD or PowerShell**:

```
cmd
CopyEdit
repadmin /removelingerobjects WIN2016DC2 <GUID-of-WIN2016DC2>
/advisory_mode
```

You can find the local DC's GUID with:

```
powershell
CopyEdit
(Get-ADDomainController -Identity $env:COMPUTERNAME).ObjectGUID
```

Then run it *for real* (after confirming safety):

```
cmd
CopyEdit
repadmin /removelingerobjects WIN2016DC2 <GUID>
```

---

### 4. ✅ Re-verify:

Run:

```
powershell
```

CopyEdit  
readmin /replsummary  
dcdiag /v

You should no longer see:

- References to WIN2016DC3
  - Replication or access errors
  - Failures under Sites and Services
- 

### Would You Like:

A **PowerShell script** that auto-detects and deletes any AD objects related to a decommissioned DC?

Or

A **report generator** to identify all stale DC objects remaining?

Let me know your preference — I'll script it for you.

### You said:

```
Get-ADObject -LDAPFilter "(cn=WIN2016DC3)" -SearchBase  
"CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Conf  
guration,DC=HomeLab,DC=TechSavvyProductions,DC=com" DistinguishedName  
Name O b j e c t C l a s s -----  
CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=H  
omeLab,DC=TechSavvyProductions,DC=com WIN2016DC3 s
```

### ChatGPT said:

Perfect — that confirms the **Server object for WIN2016DC3** still exists in **AD Sites and Services**, and is likely the reason it's still visible and causing issues.

You **already deleted the NTDS Settings object**, but the **parent CN=WIN2016DC3** remains. That's what you need to remove now.

---

✔ **Remove CN=WIN2016DC3 (Server Object) from AD**

Run this PowerShell command to delete the remaining server object:

```
powershell
CopyEdit
Remove-ADObject -Identity
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=
HomeLab,DC=TechSavvyProductions,DC=com" -Confirm:$false
```

✔ **Note:** -Recursive is **not** needed here since the NTDS Settings child is already gone.

---

 **Refresh and Verify**

Once removed:

**Check it's gone:**

```
powershell
CopyEdit
Get-ADObject -LDAPFilter "(cn=WIN2016DC3)" -SearchBase
"CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=Tech
SavvyProductions,DC=com"
```

You should get **no output** now.

**And refresh in:**

- **Active Directory Sites and Services**
- **ADUC** (dsa.msc) under Domain Controllers
- Run:

```
powershell
CopyEdit
dcdiag /v
```

readmin /showrepl

---

### Optional: Clean FSMO Role Holder References (if any)

You previously had WIN2016DC3 or WIN2016DC2 as FSMO holders. Confirm the current ones:

```
powershell
CopyEdit
netdom query fsmo
```

If any still point to WIN2016DC3, you can **seize** them via:

```
powershell
CopyEdit
Move-ADDirectoryServerOperationMasterRole -Identity "WIN2016DC2"
-OperationMasterRole 0,1,2,3,4 -Force
```

---

Let me know if you'd like a **full cleanup script** or a **PowerShell report** to check if all domain controller objects are healthy.

### You said:

```
Remove-ADObject -Identity
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=
Hom eLab,DC=TechSavvyProductions,DC=com" -Confirm:$false Remove-ADObject
: Access is denied At line:1 char:1 + Remove-ADObject -Identity
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN= ... +
~~~~~
~~ + CategoryInfo          : PermissionDenied:
(CN=WIN2016DC3,C...ductions,DC=com:ADObject) [Remove-ADObject], Unauth
orizedAccessException + FullyQualifiedErrorId :
ActiveDirectoryCmdlet:System.UnauthorizedAccessException,Microsoft.ActiveDire
ctory.Manag ement.Commands.RemoveADObject
```

### ChatGPT said:

The "**Access is denied**" error while running `Remove-ADObject` — even as an **Enterprise Admin** — strongly suggests one of the following:

---

## Likely Causes

### 1. Not running PowerShell as Administrator

Even with the right group membership, you must **run PowerShell as Administrator**.

### 2. UAC Token Restriction

Being in the **Enterprise Admins** group doesn't elevate your token automatically. You may still be running under a restricted admin token (even if your account is elevated).

### 3. Replication or lingering object conflict

If the object is **partially deleted** (tombstoned) or **lingering**, you may need to **force the deletion via ADSI Edit** or `ntdsutil`.

---

## Fix Steps

### Step 1: Reopen PowerShell with Full Privileges

- Right-click **PowerShell** or **Windows Terminal** → "**Run as Administrator**"
- Then re-run:

```
powershell
```

```
CopyEdit
```

```
Remove-ADObject -Identity
```

```
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com" -Confirm:$false
```

---

### Step 2: If it still fails → Use ADSIEdit

1. Run adsiedit.msc
  2. Navigate to:  
  
    nginx  
    CopyEdit  
    Configuration > CN=Sites > CN=HQ-Homelab > CN=Servers
  3. Right-click **CN=WIN2016DC3** > Delete
  4. Confirm deletion (and delete NTDS Settings if still present)
- 

### **Step 3: If ADSIEdit Also Fails → Use NTDSUTIL (Force Remove)**

Useful when the metadata is corrupt or cannot be removed normally.

```
bash
CopyEdit
ntdsutil
metadata cleanup
connections
connect to server WIN2016DC2
quit
select operation target
list sites
select site <# of HQ-Homelab>
list servers in site
select server <# of WIN2016DC3>
quit
remove selected server
quit
quit
```

 Don't forget to **refresh AD Sites and Services** after this.

---

 **Confirm It's Gone**

Re-run:

powershell

CopyEdit

```
Get-ADObject -LDAPFilter "(cn=WIN2016DC3)" -SearchBase  
"CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=Tech  
SavvyProductions,DC=com"
```

You should see **no results**.

---

Let me know if you'd like a **PowerShell script** to check lingering DC references or FSMO role holders.

**You said:**

```
launched PS as an administrator: Remove-ADObject -Identity  
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=  
HomeLab,DC=TechSavvyProductions,DC=com" -Confirm:$false Remove-ADObject  
: Access is denied At line:1 char:1 + Remove-ADObject -Identity  
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN= ... +  
~~~~~  
~~ + CategoryInfo          : PermissionDenied:  
(CN=WIN2016DC3,C...ductions,DC=com:ADObject) [Remove-ADObject], Unauth  
orizedAccessException + FullyQualifiedErrorId :  
ActiveDirectoryCmdlet:System.UnauthorizedAccessException,Microsoft.ActiveDire  
ctory.Manag ement.Commands.RemoveADObject
```

**ChatGPT said:**

Thanks for confirming you're running PowerShell as Administrator. Since you're still seeing Access is denied **even with elevated permissions**, here's what's likely happening:

---

 **Root Cause**

You're trying to delete a **protected object in Active Directory**, which has the **"Protect object from accidental deletion"** flag set — a common safeguard for domain controllers and critical objects.

---

## ✓ Fix (in two steps)

### 🔧 Step 1: Disable Protection

Run the following PowerShell command to remove the deletion protection flag:

```
powershell
CopyEdit
Get-ADObject
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=
HomeLab,DC=TechSavvyProductions,DC=com" |
Set-ADObject -ProtectedFromAccidentalDeletion $false
```

🔒 You must run this with administrative PowerShell and the ActiveDirectory module loaded.

---

### 🗑️ Step 2: Delete the Object

Now run the deletion:

```
powershell
CopyEdit
Remove-ADObject -Identity
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=
HomeLab,DC=TechSavvyProductions,DC=com" -Confirm:$false
```

---

### 🔍 Confirm Deletion

After deletion, verify it's gone:

```
powershell
```

CopyEdit

```
Get-ADObject -LDAPFilter "(cn=WIN2016DC3)" -SearchBase  
"CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=Tech  
SavvyProductions,DC=com"
```

You should get **no output** if it was successful.

---

Let me know if you'd like to automate deletion of related metadata entries (like NTDS settings, replication links, or orphaned connection objects).

**You said:**

```
Get-ADObject  
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=  
HomeLab,DC=TechSavvyProductions,DC=com" | >> Set-ADObject  
-ProtectedFromAccidentalDeletion $false
```

**ChatGPT said:**

Perfect — that's the exact command needed. Here's what it does and what you should do next:

---

### **What You Just Did**

This command:

```
powershell  
CopyEdit  
Get-ADObject  
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=  
HomeLab,DC=TechSavvyProductions,DC=com" |  
Set-ADObject -ProtectedFromAccidentalDeletion $false
```

 **Removed the "accidental deletion protection" flag** from the WIN2016DC3 server object in AD Sites and Services.

---

## Now, Delete the Object

Now that protection is removed, go ahead and **delete** the object:

```
powershell
CopyEdit
Remove-ADObject -Identity
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=
HomeLab,DC=TechSavvyProductions,DC=com" -Confirm:$false
```

---

## Optional: Confirm Removal

After deletion:

```
powershell
CopyEdit
Get-ADObject -LDAPFilter "(cn=WIN2016DC3)" -SearchBase
"CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=Tech
SavvyProductions,DC=com"
```

Should return **no result** if successful.

---

Would you also like to:

- Remove the NTDS Settings sub-object (if not auto-removed)?
- Clean up replication connections and AD Sites stubs?
- Confirm FSMO role transfer if WIN2016DC3 held any?

I can generate a full clean-up checklist or script next.

**You said:**

```
Get-ADObject -LDAPFilter "(cn=WIN2016DC3)" -SearchBase
"CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Con
figuration,DC=HomeLab,DC=TechSavvyProductions,DC=com"
```

## ChatGPT said:

Running this command:

```
powershell
CopyEdit
Get-ADObject -LDAPFilter "(cn=WIN2016DC3)" -SearchBase
"CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=Tech
SavvyProductions,DC=com"
```

### Purpose:

This searches for the WIN2016DC3 server object under the AD Sites and Services structure (CN=Servers,...) to verify whether it's still present.

---

### ✓ Expected Result If Object Was Removed:

No output — meaning the object was successfully deleted.

### ! Expected Result If Object Still Exists:

You'll see output like:

| DistinguishedName                                   | Name   | ObjectClass |
|-----------------------------------------------------|--------|-------------|
| -----                                               | ----   | -----       |
| CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,... |        |             |
| WIN2016DC3                                          | server |             |

---

### ▶ If It Still Exists:

Make sure you've already disabled deletion protection:

```
powershell
CopyEdit
Set-ADObject -Identity
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=
HomeLab,DC=TechSavvyProductions,DC=com" -ProtectedFromAccidentalDeletion
$false
```

Then remove it:

Remove-ADObject -Identity

```
"CN=WIN2016DC3,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com" -Confirm:$false
```

---

Let me know if you'd like:

- A script to recursively clean the entire Servers container including orphaned NTDS settings.
- Confirmation if any FSMO roles were held by WIN2016DC3.
- A follow-up on lingering metadata cleanup via ntdsutil or repadmin.

**You said:**

A script to recursively clean the entire Servers container including orphaned NTDS settings

**ChatGPT said:**

Here's a **PowerShell script** that **recursively cleans out all orphaned Domain Controller objects** under **Sites and Services** in AD — including:

- Server objects (CN=WIN2016DC3,...)
  - Associated NTDS Settings objects (CN=NTDS Settings,...)
  - Skips live/healthy DCs automatically
  - Disables ProtectedFromAccidentalDeletion before attempting deletes
  - Logs actions with color-coded feedback
- 

 **Important:**

- Run this **as a Domain Admin** from a DC or domain-joined workstation with RSAT tools.
- Have a **backup** of your AD or VM snapshot.
- Review the "detected objects" before deletion (optional confirmation step included).



## PowerShell Script: Clean Orphaned DC Objects

powershell

<#

.SYNOPSIS

Cleans orphaned Server and NTDS Settings objects from AD Sites and Services.

.DESCRIPTION

- Searches each site under CN=Sites for Server objects
- Checks if the server object refers to a valid Domain Controller
- Deletes orphaned Server and NTDS Settings objects recursively

#>

Import-Module ActiveDirectory -ErrorAction Stop

function Remove-OrphanedDCObjects {

    Write-Host "`nScanning Sites and Services for orphaned Domain  
    Controllers..." -ForegroundColor Cyan

    \$sitesPath = "CN=Sites,CN=Configuration," +  
    (Get-ADRootDSE).configurationNamingContext  
    \$sites = Get-ADObject -LDAPFilter "(objectClass=site)" -SearchBase  
    \$sitesPath

    foreach (\$site in \$sites) {  
        \$serversContainer = "CN=Servers,\$(\$site.DistinguishedName)"  
        \$servers = Get-ADObject -LDAPFilter "(objectClass=server)"  
    -SearchBase \$serversContainer -ErrorAction SilentlyContinue

        foreach (\$server in \$servers) {  
            \$dcName = \$server.Name

            \$dcExists = Get-ADDomainController -Filter { Name -eq \$dcName }  
    -ErrorAction SilentlyContinue  
            if (-not \$dcExists) {

```
Write-Host "`n[$dcName] appears to be orphaned. Attempting
cleanup..." -ForegroundColor Yellow
```

```
    # Remove NTDS Settings if present
    try {
        $ntdsPath = "CN=NTDS
Settings,$($server.DistinguishedName)"
        $ntdsObj = Get-ADObject -Identity $ntdsPath -ErrorAction
SilentlyContinue
        if ($ntdsObj) {
            Set-ADObject -Identity $ntdsObj
-ProtectedFromAccidentalDeletion $false
            Remove-ADObject -Identity $ntdsObj -Confirm:$false
            Write-Host " - Removed NTDS Settings: $ntdsPath"
-ForegroundColor DarkGray
        }
    } catch {
        Write-Warning " - Failed to remove NTDS Settings for
$dcName: $_"
    }

    # Remove the Server object
    try {
        Set-ADObject -Identity $server
-ProtectedFromAccidentalDeletion $false
        Remove-ADObject -Identity $server -Confirm:$false
        Write-Host " - Removed Server object:
 $($server.DistinguishedName)" -ForegroundColor Green
    } catch {
        Write-Warning " - Failed to remove Server object for $dcName:
$_"
    }
} else {
    Write-Host "[$dcName] is active. Skipping." -ForegroundColor
Gray
}
}
```

```
Write-Host "`nCleanup complete." -ForegroundColor Cyan  
}
```

Remove-OrphanedDCObjects

---

## How It Works

| Step | Action                                                       |
|------|--------------------------------------------------------------|
| 1.   | Scans all sites in AD Sites and Services                     |
| 2.   | Looks in each Servers container for server objects           |
| 3.   | Checks if each server object maps to a live DC               |
| 4.   | If not live, removes NTDS Settings and Server object         |
| 5.   | Handles ProtectedFromAccidentalDeletion toggle automatically |

---

## Optional Enhancements

- Add logging to a .csv or .txt file
- Add -WhatIf option to simulate
- Filter by stale DNS entries before removing

Let me know if you'd like any of those variations!

### You said:

I am still failing here in the dcdiag: Starting test: NetLogons \* Network Logons Privileges Check Verified share \\WIN2016DC2\netlogon Verified share \\WIN2016DC2\sysvol [WIN2016DC2] User credentials does not have permission to perform this operation. The account used for this test must have network logon privileges for this machine's domain. .... WIN2016DC2 failed test NetLogons

### ChatGPT said:

The NetLogons test failure in dcdiag is due to the account you're using **not having network logon privileges** on WIN2016DC2, even though you're likely running it

**locally as an Enterprise Admin.** This specific test doesn't just check for local or directory privileges — it attempts a **network logon** to the Netlogon and SYSVOL shares, which uses **different access semantics**.

---

### Layman's View

Think of it this way:

- You're sitting at the machine as an admin — but dcdiag tries to “walk in through the front door” over the network.
  - That network door requires permission that may not be granted, even to high-level users like Domain Admins unless certain policies allow it.
- 

### Technical Explanation

#### What the Test Does

The NetLogons test attempts to:

1. **Access \\DC\netlogon and \\DC\sysvol via SMB over the network**, not the local filesystem.
  2. Validate that the **authenticated user** (typically the user running dcdiag) has the **“Access this computer from the network”** privilege.
  3. Confirm that NETLOGON and SYSVOL shares are visible and responsive.
- 

### Why the Error Happens

The message:

pgsql

CopyEdit

[WIN2016DC2] User credentials does not have permission to perform this operation.

...typically results from one or more of the following:

## 1. Group Policy restriction

The user running the test **lacks the “Access this computer from the network”** privilege, which is controlled by:

pgsql

CopyEdit

Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment > Access this computer from the network

✓ Must include:

- Administrators
- Authenticated Users
- Enterprise Admins or whoever is running the test

⊘ **NOT** blocked by:

- “Deny access to this computer from the network”

## 2. Running the test under wrong context

If you RDP into the DC or use runas, ensure you're **not triggering a UAC-limited token**.

---

✓ **How to Fix**

### ◆ **Step 1: Confirm Access Rights**

On WIN2016DC2:

1. Open secpol.msc
2. Go to **Local Policies** → **User Rights Assignment**
3. Find:
  - Access this computer from the network
  - Add Authenticated Users and Administrators (if missing)

4. Check:

- o Deny access to this computer from the network — **ensure it does NOT include Enterprise Admins or your current user**

---

◆ **Step 2: Confirm Shares Exist and Are Reachable**

From another domain host:

```
cmd
CopyEdit
net view \\WIN2016DC2
```

Expected output should include:

```
vbnet
CopyEdit
Shared resources at \\WIN2016DC2
NETLOGON
SYSVOL
```

If it fails, validate that:

- File and printer sharing is enabled
- No local firewall is blocking SMB (port 445)
- The Netlogon and DFSR services are running

---

◆ **Step 3: Manually Test Network Logon**

From another DC or domain machine:

```
powershell
CopyEdit
Test-Path "\\WIN2016DC2\netlogon"
Test-Path "\\WIN2016DC2\sysvol"
```

They should return True.

---

## Optional Diagnostic

Use this command on WIN2016DC2 to show the policy:

```
powershell  
CopyEdit  
secedit /export /cfg C:\secpol.cfg  
notepad C:\secpol.cfg
```

Look under [Privilege Rights]:

```
ini  
CopyEdit  
SeNetworkLogonRight = *S-1-5-11,*S-1-5-32-544
```

- S-1-5-11 = Authenticated Users
- S-1-5-32-544 = Administrators

---

## What to Do After Fixing

After applying policy changes:

1. Run `gpupdate /force`
2. Reboot the DC if necessary
3. Re-run:

```
cmd  
CopyEdit  
dcdiag /test:NetLogons /v
```

Let me know if you'd like help exporting all local policies for audit, or a script to test Access this computer from the network rights programmatically.

**You said:**

I am promoting win2016dc4 192.168.0.233 to a domain controller but I am getting a DNS error: DNS Options A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "HomeLab.TechSavvyProductions.com". Otherwise, no action is required.

### ChatGPT said:

This **DNS Options warning** is common and **safe to ignore in most internal AD environments**, especially when promoting a **new Domain Controller (DC)** with DNS in a **single-domain forest** that doesn't require external delegation.

---



### Layman's View

When setting up a new domain controller, Windows tries to check whether it can **inform the "higher level" DNS servers** (like a public DNS server or your top-level domain authority) about the new DNS server you're adding.

But if you're just running a **private internal domain** like HomeLab.TechSavvyProductions.com, there's **no external DNS server** that knows or cares about this — and **no delegation is needed**.

This is like adding a new person to your family tree — but there's no government registry that needs to be told because it's your private family record.

---



### Technical Analysis



### Warning Message Explained

"A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found..."

This means:

- During promotion, **DCPromo** checks the parent zone of HomeLab.TechSavvyProductions.com, which is TechSavvyProductions.com, then com.
  - It fails to find a **Microsoft DNS server** authoritative for that parent zone to create a DNS delegation pointing to your new DC/DNS.
  - This is expected if:
    - You're using a **private domain** with no external DNS.
    - Or you use **non-Windows DNS servers** upstream.
    - Or there is no real TechSavvyProductions.com DNS zone to delegate from.
- 

### **When You Can Ignore This Warning**

You can **safely ignore this** if:

- This is an **internal AD DNS** zone.
  - You are **not integrating** with external/public DNS.
  - Your **existing AD DNS is functioning** correctly.
  - All internal systems use your AD DNS (e.g., 192.168.0.232 and now 192.168.0.233).
- 

### **What You Might Want To Do**

#### **Confirm DNS Is Working Internally**

After DC promotion completes:

1. Ensure both win2016dc2 and win2016dc4 have each other listed as **preferred/alternate DNS**:
  - Set DC2 → Preferred: 192.168.0.232, Alternate: 192.168.0.233
  - Set DC4 → Preferred: 192.168.0.233, Alternate: 192.168.0.232
2. Run on each DC:

```
powershell  
CopyEdit
```

nslookup \_ldap.\_tcp.dc.\_msdcs.homelab.techsavvyproductions.com

3. Run:

```
cmd
CopyEdit
repadmin /replsummary
dcdiag /v
```

These will show if replication and DNS registration succeeded.

---

### **OPTIONAL (Advanced): Create DNS Delegation**





You only need to create a **delegation in the parent zone** if:

- You own TechSavvyProductions.com externally and
- Want public DNS resolution for subdomains (like dc4.homelab.techsavvyproductions.com) and
- Your external DNS is managed by Windows DNS or supports subzone delegation.

If that's **not your case**, skip it.

---

### **Summary**

| Action                           | Required?                                                                                       | Why?                                                                         |
|----------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Fix the DNS delegation warning   |  Not needed  | Internal AD DNS does not require external delegation                         |
| Check internal DNS replication   |  Yes         | Ensures dc4 is functional and replicates properly                            |
| Configure DNS forwarders         |  Recommended | Forward unknown DNS queries to external resolvers (e.g., 8.8.8.8)            |
| Create delegation in parent zone |  Optional    | Only needed for <b>public/external DNS resolution</b> of internal subdomains |

---

## Win2016dc4

```
C:\Windows\system32>dcdiag /a /v /c /fix
```

### Directory Server Diagnosis

Performing initial setup:

Trying to find home server...

\* Verifying that the local machine Win2016dc4, is a Directory Server.

Home Server = Win2016dc4

\* Connecting to directory service on server Win2016dc4.

\* Identified AD Forest.

Collecting AD specific global data

\* Collecting site info.

Calling

```
ldap_search_init_page(hld,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyP  
roductions,DC=com,LDAP_SCOPE_SUBTREE,(objectCategory=ntDSSiteSettings),.....
```

The previous call succeeded

Iterating through the sites

Looking at base site object: CN=NTDS Site

```
Settings,CN=Mikrotek,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProdu  
ctions,DC=com
```

Getting ISTG and options for the site

Looking at base site object: CN=NTDS Site

```
Settings,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyP  
roductions,DC=com
```

Getting ISTG and options for the site

\* Identifying all servers.

Calling

ldap\_search\_init\_page(hld,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com,LDAP\_SCOPE\_SUBTREE,(objectClass=ntDSDsa),.....

The previous call succeeded....

The previous call succeeded

Iterating through the list of servers

Getting information for the server CN=NTDS

Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com

objectGuid obtained

InvocationID obtained

dnsHostname obtained

site info obtained

All the info for the server collected

Getting information for the server CN=NTDS

Settings,CN=WIN2016DC4,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com

objectGuid obtained

InvocationID obtained

dnsHostname obtained

site info obtained

All the info for the server collected

\* Identifying all NC cross-refs.

\* Found 2 DC(s). Testing 2 of them.

Done gathering initial info.

Doing initial required tests

Testing server: HQ-Homelab\WIN2016DC2

Starting test: Connectivity

\* Active Directory LDAP Services Check

Determining IP4 connectivity

\* Active Directory RPC Services Check

..... WIN2016DC2 passed test Connectivity

Testing server: HQ-Homelab\WIN2016DC4

Starting test: Connectivity

\* Active Directory LDAP Services Check

Determining IP4 connectivity

\* Active Directory RPC Services Check

..... WIN2016DC4 passed test Connectivity

Doing primary tests

Testing server: HQ-Homelab\WIN2016DC2

Starting test: Advertising

The DC WIN2016DC2 is advertising itself as a DC and having a DS.

The DC WIN2016DC2 is advertising as an LDAP server

The DC WIN2016DC2 is advertising as having a writeable directory

The DC WIN2016DC2 is advertising as a Key Distribution Center

The DC WIN2016DC2 is advertising as a time server

The DS WIN2016DC2 is advertising as a GC.

..... WIN2016DC2 passed test Advertising

Starting test: CheckSecurityError

\* Dr Auth: Beginning security errors check!

Found KDC WIN2016DC4 for domain HomeLab.TechSavvyProductions.com in site HQ-Homelab

Checking machine account for DC WIN2016DC2 on DC WIN2016DC4.

\* SPN found

:LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com

\* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com

\* SPN found :LDAP/WIN2016DC2

\* SPN found

:LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB

\* SPN found

:LDAP/60228dba-cbc8-4304-868a-28f53a302f46.\_msdcs.HomeLab.TechSavvyProductions.com

\* SPN found

:E3514235-4B06-11D1-AB04-00C04FC2DCD2/60228dba-cbc8-4304-868a-28f53a302f46/HomeLab.TechSavvyProductions.com

\* SPN found

:HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com

\* SPN found :HOST/Win2016DC2.HomeLab.TechSavvyProductions.com

\* SPN found :HOST/WIN2016DC2

\* SPN found

:HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB

\* SPN found

:GC/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com

Checking for CN=WIN2016DC2,OU=Domain

Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com in domain

DC=HomeLab,DC=TechSavvyProductions,DC=com on 2 servers

Object is up-to-date on all servers.

[WIN2016DC2] No security related replication errors were found on this DC! To target the connection to a

specific source DC use /ReplSource:<DC>.

..... WIN2016DC2 passed test CheckSecurityError

Starting test: CutoffServers

- \* Configuration Topology Aliveness Check
- \* Analyzing the alive system replication topology for  
DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.
- \* Analyzing the alive system replication topology for  
DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.
- \* Analyzing the alive system replication topology for  
CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.
- \* Analyzing the alive system replication topology for  
CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.
- \* Analyzing the alive system replication topology for  
DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.

..... WIN2016DC2 passed test CutoffServers

Starting test: FrsEvent

- \* The File Replication Service Event log test
- Skip the test because the server is running DFSR.

..... WIN2016DC2 passed test FrsEvent

Starting test: DFSREvent

The DFS Replication Event Log.

There are warning or error events within the last 24 hours after the SYSVOL has been shared. Failing SYSVOL

replication problems may cause Group Policy problems.

A warning event occurred. EventID: 0x80001A94

Time Generated: 06/21/2025 09:59:34

Event String:

The DFS Replication service has detected that no connections are configured for replication group Domain System Volume. No data is being replicated for this replication group.

Additional Information:

Replication Group ID: 7E84258A-AF73-4C40-AFAC-AB7C33CB14E7

Member ID: BF1455A5-06CA-449E-B802-D9771AEC94AB

A warning event occurred. EventID: 0x80001A94

Time Generated: 06/21/2025 10:04:35

Event String:

The DFS Replication service has detected that no connections are configured for replication group Domain System Volume. No data is being replicated for this replication group.

Additional Information:

Replication Group ID: 7E84258A-AF73-4C40-AFAC-AB7C33CB14E7

Member ID: BF1455A5-06CA-449E-B802-D9771AEC94AB

..... WIN2016DC2 passed test DFSREvent

Starting test: SysVolCheck

\* The File Replication Service SYSVOL ready test

File Replication Service's SYSVOL is ready

..... WIN2016DC2 passed test SysVolCheck

Starting test: FrsSysVol

\* The File Replication Service SYSVOL ready test

File Replication Service's SYSVOL is ready

..... WIN2016DC2 passed test FrsSysVol

Starting test: KccEvent

\* The KCC Event log test

Found no KCC errors in "Directory Service" Event log in the last 15 minutes.

..... WIN2016DC2 passed test KccEvent

Starting test: KnowsOfRoleHolders

Role Schema Owner = CN=NTDS

Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com

Role Domain Owner = CN=NTDS

Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com

Role PDC Owner = CN=NTDS

Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com

Role Rid Owner = CN=NTDS

Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com

Role Infrastructure Update Owner = CN=NTDS

Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com

..... WIN2016DC2 passed test KnowsOfRoleHolders

Starting test: MachineAccount

Checking machine account for DC WIN2016DC2 on DC WIN2016DC2.

\* SPN found

:LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com

\* SPN found :LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com  
\* SPN found :LDAP/WIN2016DC2  
\* SPN found  
:LDAP/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB  
\* SPN found  
:LDAP/60228dba-cbc8-4304-868a-28f53a302f46.\_msdcs.HomeLab.TechSavvyProductions.com  
\* SPN found  
:E3514235-4B06-11D1-AB04-00C04FC2DCD2/60228dba-cbc8-4304-868a-28f53a302f46/HomeLab.TechSavvyProductions.com  
\* SPN found  
:HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com  
\* SPN found :HOST/Win2016DC2.HomeLab.TechSavvyProductions.com  
\* SPN found :HOST/WIN2016DC2  
\* SPN found  
:HOST/Win2016DC2.HomeLab.TechSavvyProductions.com/HOMELAB  
\* SPN found  
:GC/Win2016DC2.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com

..... WIN2016DC2 passed test MachineAccount  
Starting test: NCSecDesc

- \* Security Permissions check for all NC's on DC WIN2016DC2.
- \* Security Permissions Check for  
DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(NDNC,Version 3)
- \* Security Permissions Check for  
DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(NDNC,Version 3)
- \* Security Permissions Check for

CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(Schema,Version 3)

- \* Security Permissions Check for  
CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(Configuration,Version 3)
- \* Security Permissions Check for  
DC=HomeLab,DC=TechSavvyProductions,DC=com  
(Domain,Version 3)

..... WIN2016DC2 passed test NCSecDesc  
Starting test: NetLogons

- \* Network Logons Privileges Check  
Verified share \\WIN2016DC2\netlogon  
Verified share \\WIN2016DC2\sysvol

..... WIN2016DC2 passed test NetLogons  
Starting test: ObjectsReplicated  
WIN2016DC2 is in domain DC=HomeLab,DC=TechSavvyProductions,DC=com  
Checking for CN=WIN2016DC2,OU=Domain  
Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com in domain  
DC=HomeLab,DC=TechSavvyProductions,DC=com on 2 servers  
Object is up-to-date on all servers.  
Checking for CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com in domain  
CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com on 2 servers  
Object is up-to-date on all servers.  
..... WIN2016DC2 passed test ObjectsReplicated  
Starting test: OutboundSecureChannels  
\* The Outbound Secure Channels test  
\*\* Did not run Outbound Secure Channels test because /testdomain: was not  
entered  
..... WIN2016DC2 passed test OutboundSecureChannels  
Starting test: Replications  
\* Replications Check  
\* Replication Latency Check  
DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com  
Latency information for 5 entries in the vector were ignored.  
5 were retired Invocations. 0 were either: read-only replicas and are not  
verifiably latent, or dc's no longer replicating this nc. 0 had no latency information  
(Win2K DC).  
DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com  
Latency information for 5 entries in the vector were ignored.  
5 were retired Invocations. 0 were either: read-only replicas and are not  
verifiably latent, or dc's no longer replicating this nc. 0 had no latency information  
(Win2K DC).  
CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com  
Latency information for 5 entries in the vector were ignored.  
5 were retired Invocations. 0 were either: read-only replicas and are not  
verifiably latent, or dc's no longer replicating this nc. 0 had no latency information  
(Win2K DC).  
CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com  
Latency information for 5 entries in the vector were ignored.  
5 were retired Invocations. 0 were either: read-only replicas and are not  
verifiably latent, or dc's no longer replicating this nc. 0 had no latency information  
(Win2K DC).  
DC=HomeLab,DC=TechSavvyProductions,DC=com  
Latency information for 5 entries in the vector were ignored.

5 were retired Invocations. 0 were either: read-only replicas and are not verifiably latent, or dc's no longer replicating this nc. 0 had no latency information (Win2K DC).

..... WIN2016DC2 passed test Replications

Starting test: RidManager

- \* Available RID Pool for the Domain is 15600 to 1073741823
- \* Win2016DC2.HomeLab.TechSavvyProductions.com is the RID Master
- \* DsBind with RID Master was successful
- \* rIDAllocationPool is 4100 to 4599
- \* rIDPreviousAllocationPool is 4100 to 4599
- \* rIDNextRID: 4101

..... WIN2016DC2 passed test RidManager

Starting test: Services

- \* Checking Service: EventSystem
- \* Checking Service: RpcSs
- \* Checking Service: NTDS
- \* Checking Service: DnsCache
- \* Checking Service: DFSR
- \* Checking Service: IsmServ
- \* Checking Service: kdc
- \* Checking Service: SamSs
- \* Checking Service: LanmanServer
- \* Checking Service: LanmanWorkstation
- \* Checking Service: w32time
- \* Checking Service: NETLOGON

..... WIN2016DC2 passed test Services

Starting test: SystemLog

- \* The System Event log test

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:04:18

Event String:

DCOM was unable to communicate with the computer

zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:04:18

Event String:

DCOM was unable to communicate with the computer

zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:04:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:04:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:14:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:14:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:14:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:14:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:24:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:24:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:24:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:24:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:34:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:34:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:34:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:34:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:44:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:44:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:44:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:44:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:54:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:54:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:54:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

An error event occurred. EventID: 0x0000272C

Time Generated: 06/21/2025 13:54:18

Event String:

DCOM was unable to communicate with the computer zima-server.HomeLab.TechSavvyProductions.com using any of the configured protocols; requested by PID 12ac (C:\Windows\system32\ServerManager.exe).

..... WIN2016DC2 failed test SystemLog

Starting test: Topology

- \* Configuration Topology Integrity Check

- \* Analyzing the connection topology for

DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com.

- \* Performing upstream (of target) analysis.

- \* Performing downstream (of target) analysis.

- \* Analyzing the connection topology for

DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com.

- \* Performing upstream (of target) analysis.

- \* Performing downstream (of target) analysis.

- \* Analyzing the connection topology for

CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com.

- \* Performing upstream (of target) analysis.

- \* Performing downstream (of target) analysis.

- \* Analyzing the connection topology for

CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com.

- \* Performing upstream (of target) analysis.

- \* Performing downstream (of target) analysis.

- \* Analyzing the connection topology for

DC=HomeLab,DC=TechSavvyProductions,DC=com.

- \* Performing upstream (of target) analysis.

- \* Performing downstream (of target) analysis.

..... WIN2016DC2 passed test Topology

Starting test: VerifyEnterpriseReferences

..... WIN2016DC2 passed test VerifyEnterpriseReferences

Starting test: VerifyReferences

The system object reference (serverReference)

CN=WIN2016DC2,OU=Domain

Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com and backlink on

CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com are correct.

The system object reference (serverReferenceBL)

CN=WIN2016DC2,CN=Topology,CN=Domain System

Volume,CN=DFSR-GlobalSettings,CN=System,DC=HomeLab,DC=TechSavvyProductions,DC=com

and backlink on

CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com  
are correct.

The system object reference (msDFSR-ComputerReferenceBL)  
CN=WIN2016DC2,CN=Topology,CN=Domain System  
Volume,CN=DFSR-GlobalSettings,CN=System,DC=HomeLab,DC=TechSavvyProductio  
ns,DC=com

and backlink on CN=WIN2016DC2,OU=Domain  
Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com are correct.

..... WIN2016DC2 passed test VerifyReferences  
Starting test: VerifyReplicas  
..... WIN2016DC2 passed test VerifyReplicas

Testing server: HQ-Homelab\WIN2016DC4

Starting test: Advertising

The DC WIN2016DC4 is advertising itself as a DC and having a DS.  
The DC WIN2016DC4 is advertising as an LDAP server  
The DC WIN2016DC4 is advertising as having a writeable directory  
The DC WIN2016DC4 is advertising as a Key Distribution Center  
The DC WIN2016DC4 is advertising as a time server  
The DS WIN2016DC4 is advertising as a GC.

..... WIN2016DC4 passed test Advertising

Starting test: CheckSecurityError

\* Dr Auth: Beginning security errors check!

Found KDC WIN2016DC4 for domain HomeLab.TechSavvyProductions.com in  
site HQ-Homelab

Checking machine account for DC WIN2016DC4 on DC WIN2016DC4.

\* SPN found

:LDAP/Win2016dc4.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProduc  
tions.com

\* SPN found :LDAP/Win2016dc4.HomeLab.TechSavvyProductions.com

\* SPN found :LDAP/WIN2016DC4

\* SPN found

:LDAP/Win2016dc4.HomeLab.TechSavvyProductions.com/HOMELAB

\* SPN found

:LDAP/56acdfc1-863e-49bd-a735-a8f359021d6b.\_msdcs.HomeLab.TechSavvyProducti  
ons.com

\* SPN found

:E3514235-4B06-11D1-AB04-00C04FC2DCD2/56acdfc1-863e-49bd-a735-a8f359021d  
6b/HomeLab.TechSavvyProductions.com

\* SPN found

:HOST/Win2016dc4.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProduc  
tions.com

\* SPN found :HOST/Win2016dc4.HomeLab.TechSavvyProductions.com  
\* SPN found :HOST/WIN2016DC4  
\* SPN found  
:HOST/Win2016dc4.HomeLab.TechSavvyProductions.com/HOMELAB  
\* SPN found  
:GC/Win2016dc4.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com

[WIN2016DC4] No security related replication errors were found on this DC! To target the connection to a

specific source DC use /ReplSource:<DC>.

..... WIN2016DC4 passed test CheckSecurityError

Starting test: CutoffServers

- \* Configuration Topology Aliveness Check
- \* Analyzing the alive system replication topology for DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com.
  - \* Performing upstream (of target) analysis.
  - \* Performing downstream (of target) analysis.
- \* Analyzing the alive system replication topology for DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com.
  - \* Performing upstream (of target) analysis.
  - \* Performing downstream (of target) analysis.
- \* Analyzing the alive system replication topology for CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com.
  - \* Performing upstream (of target) analysis.
  - \* Performing downstream (of target) analysis.
- \* Analyzing the alive system replication topology for CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com.
  - \* Performing upstream (of target) analysis.
  - \* Performing downstream (of target) analysis.
- \* Analyzing the alive system replication topology for DC=HomeLab,DC=TechSavvyProductions,DC=com.
  - \* Performing upstream (of target) analysis.
  - \* Performing downstream (of target) analysis.

..... WIN2016DC4 passed test CutoffServers

Starting test: FrsEvent

- \* The File Replication Service Event log test  
Skip the test because the server is running DFSR.

..... WIN2016DC4 passed test FrsEvent

Starting test: DFSREvent

The DFS Replication Event Log.

There are warning or error events within the last 24 hours after the SYSVOL has been shared. Failing SYSVOL

replication problems may cause Group Policy problems.

A warning event occurred. EventID: 0x80001780

Time Generated: 06/21/2025 09:58:33

Event String:

The DFS Replication service failed to update configuration in Active Directory Domain Services. The service will retry this operation periodically.

Additional Information:

Object Category: msDFSR-LocalSettings

Object DN: CN=DFSR-LocalSettings,CN=WIN2016DC4,OU=Domain  
Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com

Error: 2 (The system cannot find the file specified.)

Domain Controller: win2016dc2.homelab.techsavvyproductions.com

Polling Cycle: 60

A warning event occurred. EventID: 0x80001A94

Time Generated: 06/21/2025 09:58:33

Event String:

The DFS Replication service has detected that no connections are configured for replication group Domain System Volume. No data is being replicated for this replication group.

Additional Information:

Replication Group ID: 7E84258A-AF73-4C40-AFAC-AB7C33CB14E7

Member ID: D71698DD-C275-4DE9-91B1-D02554FC33B8

A warning event occurred. EventID: 0x80001206

Time Generated: 06/21/2025 09:58:33

Event String:

The DFS Replication service initialized SYSVOL at local path D:\Windows\SYSVOL\domain and is waiting to perform initial replication. The replicated folder will remain in the initial synchronization state until it has replicated with its partner Win2016DC2.HomeLab.TechSavvyProductions.com. If the server was in the process of being promoted to a domain controller, the domain controller will not advertize and function as a domain controller until this issue is resolved. This can occur if the specified partner is also in the initial synchronization state, or if sharing violations are encountered on this server or the synchronization partner. If this event occurred during the migration of SYSVOL from File Replication service (FRS) to DFS Replication, changes will not replicate out until this issue is resolved. This can cause the SYSVOL folder on this server to become out of sync with other domain controllers.

Additional Information:

Replicated Folder Name: SYSVOL Share

Replicated Folder ID: 87B7F2B4-B434-4084-AED5-08ED31F58C65

Replication Group Name: Domain System Volume

Replication Group ID: 7E84258A-AF73-4C40-AFAC-AB7C33CB14E7

Member ID: D71698DD-C275-4DE9-91B1-D02554FC33B8

Read-Only: 0

..... WIN2016DC4 passed test DFSREvent  
Starting test: SysVolCheck  
\* The File Replication Service SYSVOL ready test  
File Replication Service's SYSVOL is ready  
..... WIN2016DC4 passed test SysVolCheck  
Starting test: FrsSysVol  
\* The File Replication Service SYSVOL ready test  
File Replication Service's SYSVOL is ready  
..... WIN2016DC4 passed test FrsSysVol  
Starting test: KccEvent  
\* The KCC Event log test  
Found no KCC errors in "Directory Service" Event log in the last 15 minutes.  
..... WIN2016DC4 passed test KccEvent  
Starting test: KnowsOfRoleHolders  
Role Schema Owner = CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com  
Role Domain Owner = CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com  
Role PDC Owner = CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com  
Role Rid Owner = CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com  
Role Infrastructure Update Owner = CN=NTDS  
Settings,CN=WIN2016DC2,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com  
..... WIN2016DC4 passed test KnowsOfRoleHolders  
Starting test: MachineAccount  
Checking machine account for DC WIN2016DC4 on DC WIN2016DC4.  
\* SPN found  
:LDAP/Win2016dc4.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com  
\* SPN found :LDAP/Win2016dc4.HomeLab.TechSavvyProductions.com  
\* SPN found :LDAP/WIN2016DC4  
\* SPN found  
:LDAP/Win2016dc4.HomeLab.TechSavvyProductions.com/HOMELAB  
\* SPN found  
:LDAP/56acdfc1-863e-49bd-a735-a8f359021d6b.\_msdcs.HomeLab.TechSavvyProductions.com

\* SPN found  
:E3514235-4B06-11D1-AB04-00C04FC2DCD2/56acdfc1-863e-49bd-a735-a8f359021d6b/HomeLab.TechSavvyProductions.com

\* SPN found  
:HOST/Win2016dc4.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com

\* SPN found :HOST/Win2016dc4.HomeLab.TechSavvyProductions.com

\* SPN found :HOST/WIN2016DC4

\* SPN found  
:HOST/Win2016dc4.HomeLab.TechSavvyProductions.com/HOMELAB

\* SPN found  
:GC/Win2016dc4.HomeLab.TechSavvyProductions.com/HomeLab.TechSavvyProductions.com

..... WIN2016DC4 passed test MachineAccount

Starting test: NCSecDesc

\* Security Permissions check for all NC's on DC WIN2016DC4.

\* Security Permissions Check for  
DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(NDNC,Version 3)

\* Security Permissions Check for  
DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(NDNC,Version 3)

\* Security Permissions Check for  
CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(Schema,Version 3)

\* Security Permissions Check for  
CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com  
(Configuration,Version 3)

\* Security Permissions Check for  
DC=HomeLab,DC=TechSavvyProductions,DC=com  
(Domain,Version 3)

..... WIN2016DC4 passed test NCSecDesc

Starting test: NetLogons

\* Network Logons Privileges Check  
Verified share \\WIN2016DC4\netlogon  
Verified share \\WIN2016DC4\sysvol

..... WIN2016DC4 passed test NetLogons

Starting test: ObjectsReplicated

WIN2016DC4 is in domain DC=HomeLab,DC=TechSavvyProductions,DC=com  
Checking for CN=WIN2016DC4,OU=Domain  
Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com in domain  
DC=HomeLab,DC=TechSavvyProductions,DC=com on 2 servers  
Object is up-to-date on all servers.

Checking for CN=NTDS  
Settings,CN=WIN2016DC4,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration  
,DC=HomeLab,DC=TechSavvyProductions,DC=com in domain  
CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com on 2 servers  
Object is up-to-date on all servers.

..... WIN2016DC4 passed test ObjectsReplicated

Starting test: OutboundSecureChannels

\* The Outbound Secure Channels test

\*\* Did not run Outbound Secure Channels test because /testdomain: was not entered

..... WIN2016DC4 passed test OutboundSecureChannels

Starting test: Replications

\* Replications Check

\* Replication Latency Check

DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com

Latency information for 5 entries in the vector were ignored.

5 were retired Invocations. 0 were either: read-only replicas and are not verifiably latent, or dc's no longer replicating this nc. 0 had no latency information (Win2K DC).

DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com

Latency information for 5 entries in the vector were ignored.

5 were retired Invocations. 0 were either: read-only replicas and are not verifiably latent, or dc's no longer replicating this nc. 0 had no latency information (Win2K DC).

CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com

Latency information for 5 entries in the vector were ignored.

5 were retired Invocations. 0 were either: read-only replicas and are not verifiably latent, or dc's no longer replicating this nc. 0 had no latency information (Win2K DC).

CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com

Latency information for 5 entries in the vector were ignored.

5 were retired Invocations. 0 were either: read-only replicas and are not verifiably latent, or dc's no longer replicating this nc. 0 had no latency information (Win2K DC).

DC=HomeLab,DC=TechSavvyProductions,DC=com

Latency information for 5 entries in the vector were ignored.

5 were retired Invocations. 0 were either: read-only replicas and are not verifiably latent, or dc's no longer replicating this nc. 0 had no latency information (Win2K DC).

..... WIN2016DC4 passed test Replications

Starting test: RidManager

\* Available RID Pool for the Domain is 15600 to 1073741823

\* Win2016DC2.HomeLab.TechSavvyProductions.com is the RID Master

- \* DsBind with RID Master was successful
- \* rIDAllocationPool is 15100 to 15599
- \* rIDPreviousAllocationPool is 15100 to 15599
- \* rIDNextRID: 15100

..... WIN2016DC4 passed test RidManager

Starting test: Services

- \* Checking Service: EventSystem
- \* Checking Service: RpcSs
- \* Checking Service: NTDS
- \* Checking Service: DnsCache
- \* Checking Service: DFSR
- \* Checking Service: IsmServ
- \* Checking Service: kdc
- \* Checking Service: SamSs
- \* Checking Service: LanmanServer
- \* Checking Service: LanmanWorkstation
- \* Checking Service: w32time
- \* Checking Service: NETLOGON

..... WIN2016DC4 passed test Services

Starting test: SystemLog

- \* The System Event log test

An error event occurred. EventID: 0x00002720

Time Generated: 06/21/2025 13:56:46

Event String:

The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {8D8F4F83-3594-4F07-8369-FC3C3CAE4919} and APPID {F72671A9-012C-4725-9D2F-2A4D32D65169} to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.

..... WIN2016DC4 failed test SystemLog

Starting test: Topology

- \* Configuration Topology Integrity Check
- \* Analyzing the connection topology for DC=DomainDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.
- \* Analyzing the connection topology for DC=ForestDnsZones,DC=HomeLab,DC=TechSavvyProductions,DC=com.
- \* Performing upstream (of target) analysis.
- \* Performing downstream (of target) analysis.

\* Analyzing the connection topology for  
CN=Schema,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com.

\* Performing upstream (of target) analysis.

\* Performing downstream (of target) analysis.

\* Analyzing the connection topology for

CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com.

\* Performing upstream (of target) analysis.

\* Performing downstream (of target) analysis.

\* Analyzing the connection topology for

DC=HomeLab,DC=TechSavvyProductions,DC=com.

\* Performing upstream (of target) analysis.

\* Performing downstream (of target) analysis.

..... WIN2016DC4 passed test Topology

Starting test: VerifyEnterpriseReferences

..... WIN2016DC4 passed test VerifyEnterpriseReferences

Starting test: VerifyReferences

The system object reference (serverReference)

CN=WIN2016DC4,OU=Domain

Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com and backlink on

CN=WIN2016DC4,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com are correct.

The system object reference (serverReferenceBL)

CN=WIN2016DC4,CN=Topology,CN=Domain System

Volume,CN=DFSR-GlobalSettings,CN=System,DC=HomeLab,DC=TechSavvyProductions,DC=com

and backlink on

CN=NTDS

Settings,CN=WIN2016DC4,CN=Servers,CN=HQ-Homelab,CN=Sites,CN=Configuration,DC=HomeLab,DC=TechSavvyProductions,DC=com

are correct.

The system object reference (msDFSR-ComputerReferenceBL)

CN=WIN2016DC4,CN=Topology,CN=Domain System

Volume,CN=DFSR-GlobalSettings,CN=System,DC=HomeLab,DC=TechSavvyProductions,DC=com

and backlink on CN=WIN2016DC4,OU=Domain

Controllers,DC=HomeLab,DC=TechSavvyProductions,DC=com are correct.

..... WIN2016DC4 passed test VerifyReferences

Starting test: VerifyReplicas

..... WIN2016DC4 passed test VerifyReplicas

Starting test: DNS

Starting test: DNS

DNS Tests are running and not hung. Please wait a few minutes...

See DNS test in enterprise tests section for results

..... WIN2016DC2 failed test DNS

See DNS test in enterprise tests section for results

..... WIN2016DC4 passed test DNS

Running partition tests on : DomainDnsZones

Starting test: CheckSDRefDom

..... DomainDnsZones passed test CheckSDRefDom

Starting test: CrossRefValidation

..... DomainDnsZones passed test CrossRefValidation

Running partition tests on : ForestDnsZones

Starting test: CheckSDRefDom

..... ForestDnsZones passed test CheckSDRefDom

Starting test: CrossRefValidation

..... ForestDnsZones passed test CrossRefValidation

Running partition tests on : Schema

Starting test: CheckSDRefDom

..... Schema passed test CheckSDRefDom

Starting test: CrossRefValidation

..... Schema passed test CrossRefValidation

Running partition tests on : Configuration

Starting test: CheckSDRefDom

..... Configuration passed test CheckSDRefDom

Starting test: CrossRefValidation

..... Configuration passed test CrossRefValidation

Running partition tests on : HomeLab

Starting test: CheckSDRefDom

..... HomeLab passed test CheckSDRefDom

Starting test: CrossRefValidation

..... HomeLab passed test CrossRefValidation

Running enterprise tests on : HomeLab.TechSavvyProductions.com

Starting test: DNS

Test results for domain controllers:

DC: Win2016DC2.HomeLab.TechSavvyProductions.com

Domain: HomeLab.TechSavvyProductions.com

TEST: Authentication (Auth)

Authentication test: Successfully completed

TEST: Basic (Basc)

Error: No WMI connectivity

[Error details: 0x80070005 (Type: HRESULT - Facility: Win32, Description: Access is denied.) - Connection to WMI server failed]

No host records (A or AAAA) were found for this DC

DC: Win2016dc4.HomeLab.TechSavvyProductions.com

Domain: HomeLab.TechSavvyProductions.com

TEST: Authentication (Auth)

Authentication test: Successfully completed

TEST: Basic (Basc)

The OS Microsoft Windows Server 2016 Standard (Service Pack level: 0.0) is supported.

NETLOGON service is running

kdc service is running

DNSCACHE service is running

DNS service is running

DC is a DNS server

Network adapters information:

Adapter [00000000] Microsoft Hyper-V Network Adapter:

MAC address is 00:15:5D:00:6A:12

IP Address is static

IP address: 192.168.0.233, fe80::60a1:d065:4bea:e336

DNS servers:

192.168.0.231 (<name unavailable>) [Valid]

192.168.0.233 (WIN2016DC4) [Valid]

Warning:

192.168.0.1 (<name unavailable>) [Invalid]

Warning: adapter [00000000] Microsoft Hyper-V Network Adapter has invalid DNS server:

192.168.0.1 (<name unavailable>)

127.0.0.1 (WIN2016DC4) [Valid]

The A host record(s) for this DC was found

The SOA record for the Active Directory zone was found

The Active Directory zone on this DC/DNS server was found primary

Root zone on this DC/DNS server was not found

TEST: Forwarders/Root hints (Forw)

Recursion is enabled

Forwarders Information:

1.1.1.1 (<name unavailable>) [Valid]

9.9.9.9 (<name unavailable>) [Valid]

TEST: Delegations (Del)

Delegation information for the zone: HomeLab.TechSavvyProductions.com.

Delegated domain name: \_msdcs.HomeLab.TechSavvyProductions.com.

Error: DNS server: win2016dc1.homelab.techsavvyproductions.com.

IP:<Unavailable>

[Missing glue A record]

[Error details: 9714 (Type: Win32 - Description: DNS name does not exist.)]

TEST: Dynamic update (Dyn)

Test record dcdiag-test-record added successfully in zone  
HomeLab.TechSavvyProductions.com

Test record dcdiag-test-record deleted successfully in zone  
HomeLab.TechSavvyProductions.com

TEST: Records registration (RReg)

Network Adapter [00000000] Microsoft Hyper-V Network Adapter:

Matching CNAME record found at DNS server 192.168.0.231:

56acdfc1-863e-49bd-a735-a8f359021d6b.\_msdcs.HomeLab.TechSavvyProductions.com

Matching A record found at DNS server 192.168.0.231:

Win2016dc4.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:

\_ldap.\_tcp.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:

\_ldap.\_tcp.f78e894e-5fdb-4819-8919-f0da63fd69d9.domains.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:

\_kerberos.\_tcp.dc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:  
\_ldap.\_tcp.dc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:  
\_kerberos.\_tcp.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:  
\_kerberos.\_udp.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:  
\_kpasswd.\_tcp.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:  
\_ldap.\_tcp.HQ-Homelab.\_sites.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:

\_kerberos.\_tcp.HQ-Homelab.\_sites.dc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:

\_ldap.\_tcp.HQ-Homelab.\_sites.dc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:  
\_kerberos.\_tcp.HQ-Homelab.\_sites.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:  
\_ldap.\_tcp.gc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching A record found at DNS server 192.168.0.231:  
gc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:  
\_gc.\_tcp.HQ-Homelab.\_sites.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.231:

\_ldap.\_tcp.HQ-Homelab.\_sites.gc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching CNAME record found at DNS server 192.168.0.233:

56acdfc1-863e-49bd-a735-a8f359021d6b.\_msdcs.HomeLab.TechSavvyProductions.com

Matching A record found at DNS server 192.168.0.233:  
Win2016dc4.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_ldap.\_tcp.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:

\_ldap.\_tcp.f78e894e-5fdb-4819-8919-f0da63fd69d9.domains.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_kerberos.\_tcp.dc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_ldap.\_tcp.dc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_kerberos.\_tcp.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_kerberos.\_udp.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_kpasswd.\_tcp.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_ldap.\_tcp.HQ-Homelab.\_sites.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:

\_kerberos.\_tcp.HQ-Homelab.\_sites.dc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:

\_ldap.\_tcp.HQ-Homelab.\_sites.dc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_kerberos.\_tcp.HQ-Homelab.\_sites.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_ldap.\_tcp.gc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching A record found at DNS server 192.168.0.233:

gc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_gc.\_tcp.HQ-Homelab.\_sites.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:

\_ldap.\_tcp.HQ-Homelab.\_sites.gc.\_msdcs.HomeLab.TechSavvyProductions.com

Warning:

Missing CNAME record at DNS server 192.168.0.1:

56acdfc1-863e-49bd-a735-a8f359021d6b.\_msdcs.HomeLab.TechSavvyProductions.com

[Error details: 9003 (Type: Win32 - Description: DNS name does not exist.)]

Warning:

Missing A record at DNS server 192.168.0.1:

Win2016dc4.HomeLab.TechSavvyProductions.com

[Error details: 9003 (Type: Win32 - Description: DNS name does not exist.)]

Error:

Missing SRV record at DNS server 192.168.0.1:

\_ldap.\_tcp.HomeLab.TechSavvyProductions.com

[Error details: 9003 (Type: Win32 - Description: DNS name does not exist.)]

Error:

Missing SRV record at DNS server 192.168.0.1:

\_ldap.\_tcp.f78e894e-5fdb-4819-8919-f0da63fd69d9.domains.\_msdcs.HomeLab.TechSavvyProductions.com

[Error details: 9003 (Type: Win32 - Description: DNS name does not exist.)]

Error:

Missing SRV record at DNS server 192.168.0.1:

\_kerberos.\_tcp.dc.\_msdcs.HomeLab.TechSavvyProductions.com

[Error details: 9003 (Type: Win32 - Description: DNS name does not exist.)]

Error:

Missing SRV record at DNS server 192.168.0.1:  
\_ldap.\_tcp.dc.\_msdcs.HomeLab.TechSavvyProductions.com  
[Error details: 9003 (Type: Win32 - Description: DNS name does not  
exist.)]

Error:  
Missing SRV record at DNS server 192.168.0.1:  
\_kerberos.\_tcp.HomeLab.TechSavvyProductions.com  
[Error details: 9003 (Type: Win32 - Description: DNS name does not  
exist.)]

Error:  
Missing SRV record at DNS server 192.168.0.1:  
\_kerberos.\_udp.HomeLab.TechSavvyProductions.com  
[Error details: 9003 (Type: Win32 - Description: DNS name does not  
exist.)]

Error:  
Missing SRV record at DNS server 192.168.0.1:  
\_kpasswd.\_tcp.HomeLab.TechSavvyProductions.com  
[Error details: 9003 (Type: Win32 - Description: DNS name does not  
exist.)]

Error:  
Missing SRV record at DNS server 192.168.0.1:  
\_ldap.\_tcp.HQ-Homelab.\_sites.HomeLab.TechSavvyProductions.com  
[Error details: 9003 (Type: Win32 - Description: DNS name does not  
exist.)]

Error:  
Missing SRV record at DNS server 192.168.0.1:  
\_kerberos.\_tcp.HQ-Homelab.\_sites.dc.\_msdcs.HomeLab.TechSavvyProductions.com  
[Error details: 9003 (Type: Win32 - Description: DNS name does not  
exist.)]

Error:  
Missing SRV record at DNS server 192.168.0.1:  
\_ldap.\_tcp.HQ-Homelab.\_sites.dc.\_msdcs.HomeLab.TechSavvyProductions.com  
[Error details: 9003 (Type: Win32 - Description: DNS name does not  
exist.)]

Error:

Missing SRV record at DNS server 192.168.0.1:  
\_kerberos.\_tcp.HQ-Homelab.\_sites.HomeLab.TechSavvyProductions.com  
[Error details: 9003 (Type: Win32 - Description: DNS name does not  
exist.)]

Error:  
Missing SRV record at DNS server 192.168.0.1:  
\_ldap.\_tcp.gc.\_msdcs.HomeLab.TechSavvyProductions.com  
[Error details: 9003 (Type: Win32 - Description: DNS name does not  
exist.)]

Warning:  
Missing A record at DNS server 192.168.0.1:  
gc.\_msdcs.HomeLab.TechSavvyProductions.com  
[Error details: 9003 (Type: Win32 - Description: DNS name does not  
exist.)]

Error:  
Missing SRV record at DNS server 192.168.0.1:  
\_gc.\_tcp.HQ-Homelab.\_sites.HomeLab.TechSavvyProductions.com  
[Error details: 9003 (Type: Win32 - Description: DNS name does not  
exist.)]

Error:  
Missing SRV record at DNS server 192.168.0.1:  
\_ldap.\_tcp.HQ-Homelab.\_sites.gc.\_msdcs.HomeLab.TechSavvyProductions.com  
[Error details: 9003 (Type: Win32 - Description: DNS name does not  
exist.)]

Matching CNAME record found at DNS server 192.168.0.233:  
56acdfc1-863e-49bd-a735-a8f359021d6b.\_msdcs.HomeLab.TechSavvyProductions.co  
m

Matching A record found at DNS server 192.168.0.233:  
Win2016dc4.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_ldap.\_tcp.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:

\_ldap.\_tcp.f78e894e-5fdb-4819-8919-f0da63fd69d9.domains.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_kerberos.\_tcp.dc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_ldap.\_tcp.dc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_kerberos.\_tcp.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_kerberos.\_udp.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_kpasswd.\_tcp.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_ldap.\_tcp.HQ-Homelab.\_sites.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:

\_kerberos.\_tcp.HQ-Homelab.\_sites.dc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:

\_ldap.\_tcp.HQ-Homelab.\_sites.dc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_kerberos.\_tcp.HQ-Homelab.\_sites.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_ldap.\_tcp.gc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching A record found at DNS server 192.168.0.233:  
gc.\_msdcs.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:  
\_gc.\_tcp.HQ-Homelab.\_sites.HomeLab.TechSavvyProductions.com

Matching SRV record found at DNS server 192.168.0.233:

\_ldap.\_tcp.HQ-Homelab.\_sites.gc.\_msdcs.HomeLab.TechSavvyProductions.com

Error: Record registrations cannot be found for all the network adapters

Summary of test results for DNS servers used by the above domain controllers:

DNS server: 192.168.0.1 (<name unavailable>)

1 test failure on this DNS server

Name resolution is not functional.

\_ldap.\_tcp.HomeLab.TechSavvyProductions.com. failed on the DNS server 192.168.0.1

[Error details: 9003 (Type: Win32 - Description: DNS name does not exist.)]

DNS server: 1.1.1.1 (<name unavailable>)

All tests passed on this DNS server

DNS server: 192.168.0.231 (<name unavailable>)

All tests passed on this DNS server

Name resolution is functional. \_ldap.\_tcp SRV record for the forest root domain is registered

DNS server: 192.168.0.233 (WIN2016DC4)

All tests passed on this DNS server

Name resolution is functional. \_ldap.\_tcp SRV record for the forest root domain is registered

DNS server: 9.9.9.9 (<name unavailable>)

All tests passed on this DNS server

Summary of DNS test results:

Auth Basc Forw Del Dyn RReg Ext

---

|                                          |      |      |      |      |      |      |     |     |
|------------------------------------------|------|------|------|------|------|------|-----|-----|
| Domain: HomeLab.TechSavvyProductions.com |      |      |      |      |      |      |     |     |
| Win2016DC2                               | PASS | FAIL | n/a  | n/a  | n/a  | n/a  | n/a | n/a |
| Win2016dc4                               | PASS | WARN | PASS | FAIL | PASS | FAIL | n/a | n/a |

..... HomeLab.TechSavvyProductions.com failed test DNS  
Starting test: LocatorCheck  
GC Name: \\Win2016dc4.HomeLab.TechSavvyProductions.com  
Locator Flags: 0xe001f1fc  
PDC Name: \\Win2016DC2.HomeLab.TechSavvyProductions.com  
Locator Flags: 0xe003f3fd

Time Server Name: \\Win2016dc4.HomeLab.TechSavvyProductions.com  
Locator Flags: 0xe001f1fc  
Preferred Time Server Name:  
\\Win2016DC2.HomeLab.TechSavvyProductions.com  
Locator Flags: 0xe003f3fd  
KDC Name: \\Win2016dc4.HomeLab.TechSavvyProductions.com  
Locator Flags: 0xe001f1fc  
..... HomeLab.TechSavvyProductions.com passed test LocatorCheck  
Starting test: FsmoCheck  
GC Name: \\Win2016dc4.HomeLab.TechSavvyProductions.com  
Locator Flags: 0xe001f1fc  
PDC Name: \\Win2016DC2.HomeLab.TechSavvyProductions.com  
Locator Flags: 0xe003f3fd  
Time Server Name: \\Win2016dc4.HomeLab.TechSavvyProductions.com  
Locator Flags: 0xe001f1fc  
Preferred Time Server Name:  
\\Win2016DC2.HomeLab.TechSavvyProductions.com  
Locator Flags: 0xe003f3fd  
KDC Name: \\Win2016dc4.HomeLab.TechSavvyProductions.com  
Locator Flags: 0xe001f1fc  
..... HomeLab.TechSavvyProductions.com passed test FsmoCheck  
Starting test: Intersite  
Skipping site Mikrotek, this site is outside the scope provided by the command line arguments provided.  
Doing intersite inbound replication test on site HQ-Homelab:  
  Locating & Contacting Intersite Topology Generator (ISTG) ...  
  The ISTG for site HQ-Homelab is: WIN2016DC2.  
  Checking for down bridgeheads ...  
  Doing in depth site analysis ...  
  All expected sites and bridgeheads are replicating into site HQ-Homelab.  
..... HomeLab.TechSavvyProductions.com passed test Intersite

**C:\Windows\system32>repadmin /replsummary**

Replication Summary Start Time: 2025-06-21 14:18:15

Beginning data collection for replication summary, this may take awhile:

.....

| Source DSA | largest delta | fails/total | %% | error |
|------------|---------------|-------------|----|-------|
| WIN2016DC2 | 15m:58s       | 0 / 5       | 0  |       |
| WIN2016DC4 | 15m:58s       | 0 / 5       | 0  |       |

| Destination DSA | largest delta | fails/total | %% | error |
|-----------------|---------------|-------------|----|-------|
| WIN2016DC2      | 15m:58s       | 0 / 5       | 0  |       |
| WIN2016DC4      | 15m:58s       | 0 / 5       | 0  |       |