1: Define The Problem
Precisely state what the problem is – and what it isn’t

2: Gather Detailed Information
What doesn’t work? What does work? What changed? Do others have this problem?

3: Consider Probable Cause For The Failure

4: Devise A Plan To Test The Hypothesis

5: Observe The Test Results

6: Success?

7: Choose Next Most Likely Hypothesis

8: Document Changes
Hold post mortem, update production docs

End

Have you exhausted the most likely (i.e. Occam’s) causes?

Troubleshoot From The Wire Up. Physical, network, name resolution, OS, authentication/authorization, application

Yes

No

Occam’s Razor: The simplest answer is usually the correct one.
Client experiencing error?

Y

Error Joining Domain?

N

Error Finding / Contacting DC?

N

Error Authentication (e.g. password) Related?

N

Slow Logon?

N

Group Policy Not applied?

N

Error Authorization Related?

N

DC experiencing Error

DC won't boot normally?

Boots, but local NTDS error?

AD changes not showing up everywhere?

DS Replication?

SYSVOL Replication

FRS?

DFS-R

What else?
Network Troubleshooting

**Network Issues**

- Ping a computer on this computer's subnet?
  - Success?
    - Y: Confirm Host IP, Subnet / DG, DNS config
    - N: Not receiving IP address from DHCP
  - N: Ping a computer on another subnet?
    - Y: Confirm Host IP, Subnet / DG, DNS config
    - N: DHCP client & 169.254.x.x IP address?
      - Y: Run IPCONFIG /ALL
      - N: Not receiving IP address from DHCP
        - Y: Run "Diagnose & Repair"
        - N: Tracert / NetMon / Wireshark
          - Y: End
          - N: Windows 2003?
            - Y: Run NETDIAG
            - N: Success?
              - Y: End
              - N: Vista+ / WS08+?
                - Y: Run NETSH DIAG GUI
                - N: Not receiving IP address from DHCP
                  - Y: Run "Diagnose & Repair"
                  - N: Tracer / NetMon / Wireshark
                    - Y: End
                    - N: Windows XP?
                      - Y: Not receiving IP address from DHCP
                      - N: Windows 2003?
Client - DC Name Resolution Issues

Does the client’s DNS server respond to pings?

Y

Is the primary DNS server correct?

Y

Configure correct DNS server

N

Can the client resolve their domain? NSLOOKUP <FQDN>.

Y

DNS Server Problem (already passed network tests)

N

N

Can the client resolve their domain? NSLOOKUP <FQDN>.

Y

DNS Server Configuration Problem

N

Are all name servers listed available?

Y

Check SRV records for the domain (nslookup -q=srv _ldap_tcp.dc._msdcs.<FQDN>)

N

Success? (List of DC SRV records)

Y

Can client get a DC? (NLTEST / DSGETDC:<domain>)

N

Reset secure channel (NLTEST / SC_RESET:<domain>)

N

Return

Correct DC errors or DNS configuration

Client-DC Name Resolution

(Assumes network testing passed)
AD Database Troubleshooting

Check DB Integrity: NTDSUTIL, FILE, INTEGRITY

Success?

Y

Run semantic database analysis: NTDSUTIL, SEMANTIC DATABASE ANALYSIS, VERBOSE ON, GO

Success?

Reboot into normal mode

Y

Perform database recovery: NTDSUTIL, FILES, RECOVER

Success?

N

Recoverable Errors?

N

Rebuild

N

Reboot Into DSRM

N

"Net Stop NTDS"

Windows 2008?

N

End

Y

N

Run semantic database analysis with fixup: NTDSUTIL, SEMANTIC DATABASE ANALYSIS, VERBOSE ON, GO FIXUP

Success?

Y

N

Rebuild
Customer reports GPO is not being applied to client

Run RSOP.MSC on client, examine results

Run GPMC, review Results report

Is the setting listed?

Check:
- GPO Inheritance
- Replication
- Group Policy Refresh
- Asynchronous Processing
- Client Side Extensions
- Loopback Processing

Has policy been applied?

Check:
- Security Filtering
- Disabled GPO
- Inaccessible Data
- Empty GPO
- WMI Filter

Is the GPO listed in the Denied List?

Check:
- Replication
- Group Policy Refresh
- Operating System Support
- Slow Link

Check:
- Scope of Management
- Replication
- Group Policy Refresh
- Network Connectivity

End