SOP-AD-001_Domain_Troubleshooting_v1.0.0

SOP-AD-001_Domain_Troubleshooting_v1.0.0

SOP-AD-001: Active Directory Domain Connection Troubleshooting

Version: 1.1 **Status:** Final **Author:** System Administrator **Date:** 2025-12-02

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to provide a systematic process for diagnosing and resolving network connectivity issues between an endpoint (computer or user) and the Active Directory (AD) domain controller.

2.0 Scope

This procedure applies to any domain-joined computer that is unable to communicate with the Active Directory domain. This includes issues related to user logons, accessing network resources, or receiving group policy updates.

3.0 Prerequisites

- Administrative privileges on the affected endpoint machine.
- Knowledge of the network's Domain Controller (DC) IP address(es).
- Access to firewall configuration, if applicable.
- Familiarity with basic Windows networking commands (`ipconfig`, `nltest`).

4.0 Procedure

4.1 Initial DNS and Network Configuration Diagnostics

1. **Open Command Prompt:** On the affected machine, open a Command Prompt window with administrative privileges.

2. **Gather Network Information:** Execute the following command to display the current network configuration: `cmd ipconfig /all`
3. **Analyze Configuration:** Review the output and verify the following:
   - The machine has a valid IP address for its subnet.
   - Note whether the network adapter is configured for **DHCP** or a **Static IP**.
   - Identify the listed DNS servers.

4.2 Correcting DNS Configuration

1. **Verify DNS Server Order:** The DNS server settings are critical for domain communication. Ensure they are configured in the correct order of priority:
   - **Primary DNS:** Must be the primary Domain Controller's IP address.
   - **Secondary DNS:** Should be the secondary Domain Controller's IP address, if one exists. If not, this can be the circuit provider's DNS.
   - **Tertiary DNS:** A public DNS server (e.g., `8.8.8.8`) can be used as a final fallback.

   Example Hierarchy:
   - Primary: `192.168.1.1` (Primary DC)
   - Secondary: `192.168.1.2` (Secondary DC)
   - Tertiary: `142.190.111.111` (ISP DNS)
2. **Apply DNS Changes:** If the DNS settings are incorrect, update them in the machine's network adapter properties.
3. **Flush DNS Cache:** After making changes, clear the DNS resolver cache: `cmd ipconfig /flushdns`
4. **Re-register DNS:** Force the client to re-register its DNS records: `cmd ipconfig /registerdns`
5. **Confirm Changes:** Run `ipconfig /all` again to ensure the new settings have been applied.

4.3 Firewall DNS Configuration

1. If a network firewall is in place, access its management interface.
2. Verify that the DNS settings configured on the firewall match the required DNS hierarchy for the domain (i.e., pointing to the internal Domain Controllers).

4.4 Time Synchronization Verification (CRITICAL for Kerberos)

> **IMPORTANT:** Kerberos authentication requires time to be synchronized within 5 minutes between the client and domain controller. Time skew is a common cause of authentication failures.

1. **Check Current Time Configuration:** `cmd w32tm /query /status`

2. **Verify Time Source:** Ensure the endpoint is synchronizing with a domain controller: `cmd w32tm /query /source` Expected output should show

a domain controller, not `Local CMOS Clock` or `Free-running System Clock`.

3. **Force Time Resync:** If time is out of sync: `cmd w32tm /resync /force`
4. **Check Time Skew:** Compare time with domain controller: `cmd net time \\<domain_controller_name>`

4.5 Secure Channel Verification

1. **Test Secure Channel:** Verify the trust relationship between the computer and domain: `cmd nltest /sc_verify:<domain_name>` A successful output shows `NERR_Success`. If it fails, the computer account password may be out of sync.
2. **Reset Computer Account (if secure channel fails):** `cmd netdom resetpwd /server:<domain_controller> /userd:<domain>\administrator /passwordd:*` You will be prompted for the administrator password. A reboot is required after resetting.

5.0 Verification

1. **Verify DNS SRV Records:** Confirm the client can locate domain controllers via DNS: `cmd nslookup -type=SRV _ldap._tcp.dc._msdcs.<domain_name>` A successful response lists the domain controllers. If this fails, DNS is not properly configured.
2. **Test Domain Controller Discovery:** Run the following command to verify domain controller discovery: `cmd nltest /dsgetdc:<domain_name>`
3. **Analyze Output:** A successful output will show the name of the DC that responded and confirm a connection. If the command fails or times out, the endpoint is still unable to communicate with the DC, and further troubleshooting is required.
4. **Test Group Policy:** Force a Group Policy refresh to confirm full domain connectivity: `cmd gpupdate /force`
5. **Check Event Logs:** Review the following logs for authentication errors:
   - Event Viewer > Windows Logs > System (look for Netlogon errors)
   - Event Viewer > Windows Logs > Security (look for logon failures)

6.0 Troubleshooting Quick Reference

Symptom	Likely Cause	Resolution
"The trust relationship between this workstation and the primary domain failed"	Secure channel broken	Run `nltest /sc_verify:<domain>`. If failed, reset with `netdom resetpwd` and reboot.
"There are currently no logon servers available"	DNS misconfiguration	Verify DNS points to DC. Run `nslookup -type=SRV _ldap._tcp.dc._msdcs.<domain>`.
"The security database on the server does not have a computer account"	Computer account deleted or missing	Rejoin the computer to the domain.
Kerberos errors in Event Log	Time skew > 5 minutes	Run `w32tm /resync /force`. Verify with `w32tm /query /status`.
Group Policy not applying	DC unreachable or DNS issue	Run `gpupdate /force`. Check `gpresult /r` for errors.
Intermittent logon failures	Multiple DCs with replication issues	Run `repadmin /showrepl` on DC to check replication health.

7.0 Additional Considerations

- **Network Equipment Power Cycle:** If settings have been changed but are not propagating, a restart or power cycle of network switches, routers, and the affected endpoint may be required to force the changes to apply.
- **Firewall IP Reservation:** In environments with a firewall managing DHCP, it may be necessary to create a static IP reservation for the Domain Controller(s) to ensure their IP addresses do not change.
- **DHCP Lease Scope:** Adjustments to the DHCP lease scope on the firewall or DHCP server may be necessary in specific cases, such as network segmentation or IP address exhaustion. This should be evaluated on a case-by-case basis.

8.0 Related Documents

- SOP-AD-002: Adding Mac Device to Active Directory Domain
- SOP-HYB-001: Hybrid Active Directory Components

9.0 Revision History

Version	Date	Author	Description
1.0	2025-12-02	System Administrator	Initial document creation.
1.1	2025-12-29	Jeremy Smith	SME Review: Added DNS flush/registerdns steps. Added Section 4.4 (Time Sync for Kerberos). Added Section 4.5 (Secure Channel Verification). Enhanced Section 5.0 with SRV records, gpupdate, and Event Log checks. Added troubleshooting quick reference table.

End of Document