🔍 L2 Server Diagnostics Guide

Comprehensive Windows Server Troubleshooting for L2 Support

Version 4.0 - Enhanced

Author: Syed Rizvi | Last Updated: January 2026

📋 Overview

This guide provides L2 support staff with safe, effective tools for diagnosing and resolving common Windows Server issues.

✅ AUDIT Script (Read-Only)

Safely collects diagnostic information without making any changes. Creates CSV and HTML reports.
25 comprehensive checks!

SAFE FOR L2

🔧 FIX Script (With Prompts)

Fixes common issues with prompts before each action. 12 safe fix operations.

REQUIRES APPROVAL

✓ **SAFE:** Both scripts are designed to be safe for L2 use. No dangerous commands like KILL, PURGE machine accounts, or forceful resets are included.

📁 **Reports save to TWO locations:**

1. Desktop (default)
2. C:\L2_Reports (always)

📜 Scripts

1. Audit Script (L2-ServerDiagnostics-Audit-v4.ps1)

Run this FIRST to identify issues.

```
# Run the audit script (READ-ONLY) .\L2-ServerDiagnostics-Audit-v4.ps1 # Specify custom output path .\L2-ServerDiagnostics-Audit-v4.ps1 -OutputPath "C:\Reports"
```

Output Files (saved to BOTH locations):

- `L2_Audit_COMPUTERNAME_timestamp.csv` - For Excel analysis
- `L2_Audit_COMPUTERNAME_timestamp.html` - Visual report

2. Fix Script (L2-ServerDiagnostics-Fix-v4.ps1)

Run this AFTER the audit to fix identified issues.

```
# Run the fix script (PROMPTS before each action) .\L2-ServerDiagnostics-Fix-v4.ps1
```

> ⚠️ **IMPORTANT:** The fix script will PROMPT you before each action. Read carefully and approve only what you understand.

🔍 25 Checks Performed

#	Category	Check	Why It Matters
1	System	System Information	Basic server info, uptime
2	Activation	Windows Activation NEW	Unlicensed = compliance issue
3	Domain	Trust Relationship	Broken trust = users can't log in
4	GPO	Group Policy Status	GPO errors cause policy failures
5	Replication	AD Replication (DC only)	Replication failures affect domain
6	CPU	CPU Usage NEW	High CPU = performance problems
7	Processes	Top Processes NEW	Shows what's eating CPU/Memory
8	Memory	RAM Usage	High memory = performance issues
9	PageFile	Page File Usage NEW	Low page file = crashes
10	Disk	Disk Space	Low space causes failures

11	Services	Critical Services	Stopped services = issues
12	NIC Team	NIC Teaming Status NEW	Broken team = network issues
13	SSL Certs	Certificate Expiration NEW	Expired certs = app outages
14	Security	Security Tools (Trellix, Trend, Nessus)	Must be running for compliance
15	Time	Time Synchronization	Time drift breaks Kerberos
16	Reboot	Pending Reboot	May cause unstable behavior
17	RDP	RDP Configuration	RDP issues = no remote access
18	Firewall	Firewall Status	Firewall state check
19	Tasks	Failed Scheduled Tasks NEW	Broken tasks = missed jobs
20	Backup	Windows Backup Status NEW	Is backup working?
21	Security	Failed Login Attempts NEW	Brute force detection
22	Events	Last 20 Event Errors	Recent system problems
23	Network	Network Connectivity	

			DC/DNS reachability
24	Patches	Patch Status	Unpatched = vulnerable
25	Summary	Summary Statistics	Overall health score

🛡️ Security Tools Checked

Tenable Nessus Agent

Service: `Tenable Nessus Agent`
Checks: Running status + Link status

Trellix (McAfee)

Services: `macmnsvc, masvc, mfefire, mfemms, McShield`
Checks: 7 services + ePO connection

Trend Micro

Services: `ds_agent, TmListen, ntrtscan`
Checks: 6 services + DSA Manager

CrowdStrike Falcon

Service: `CSFalconService`

Windows Defender

Service: `WinDefend`

Nessus Agent Commands

```
# Check Nessus Agent status cd "C:\Program Files\Tenable\Nessus Agent" .\nessuscli.exe agent status # If not linked (requires
```

```
linking key from Tenable.io) .\nessuscli.exe agent link --
key=YOUR_KEY --host=cloud.tenable.com --port=443
```

🆕 New in Version 4.0

✅ Windows Activation Check

Detects if Windows is licensed or not - compliance requirement

✅ CPU Usage Monitoring

Real-time CPU percentage with warning thresholds (80%/90%)

✅ Top Processes

Shows top 5 CPU and top 5 Memory consuming processes

✅ Page File Usage

Checks virtual memory/page file health

✅ NIC Teaming Status

Checks if NIC teams are UP and all members active

✅ SSL Certificate Expiration

Finds expired and expiring certificates (30/90 day warning)

✅ Failed Scheduled Tasks

Lists tasks that failed in the last 7 days

✅ Windows Backup Status

Checks if Windows Server Backup is successful

✅ Failed Login Attempts

Security check - detects brute force attempts (24h)

✅ Dual Location Saving

Reports save to Desktop AND C:\L2_Reports

🔧 Common Issues & Fixes

Issue: Trust Relationship Broken

Symptoms

- "The trust relationship between this workstation and the primary domain failed"
- Users cannot log in with domain accounts

Fix (L2 Can Do)

Run the FIX script and approve Trust Repair, OR:

```
Test-ComputerSecureChannel -Repair -Credential (Get-Credential)
```

Issue: High CPU Usage

Symptoms

- Server slow/unresponsive
- CPU > 80% in audit report

Investigation (L2 Can Do)

```
# Check top CPU processes Get-Process | Sort-Object CPU -Descending | Select -First 10 # Check specific process Get-Process -Name "processname" | Format-List *
```

Issue: SSL Certificate Expired

Symptoms

- Application errors

- HTTPS failures
- Certificate warnings in audit

Check (L2 Can Do)

```
# List expiring certificates Get-ChildItem Cert:
\LocalMachine\My | Where-Object { $_.NotAfter -lt (Get-
Date).AddDays(30) } | Select Subject, NotAfter
```

Note: Certificate renewal typically requires L3 or app team.

Issue: Failed Logins (Possible Brute Force)

Symptoms

- >50 failed logins in 24h in audit report
- Account lockouts

Investigation (L2 Can Do)

```
# Get failed login details Get-WinEvent -FilterHashtable
@{LogName='Security'; Id=4625} -MaxEvents 50 | Select
TimeCreated, Message
```

Escalate to Security team if >50 attempts!

⚡ Quick Reference Commands

Safe Commands for L2

Purpose	Command
Check trust	`Test-ComputerSecureChannel`
Refresh GPO	`gpupdate /force`
Check GPO	`gpresult /r`
Sync time	`w32tm /resync /force`
Flush DNS	`Clear-DnsClientCache`
Register DNS	`ipconfig /registerdns`
Check services	`Get-Service | Where Status -eq Stopped`
Start service	`Start-Service -Name "ServiceName"`
Check CPU	`Get-WmiObject Win32_Processor | Select LoadPercentage`
Check memory	`Get-WmiObject Win32_OperatingSystem | Select FreePhysicalMemory`
Check disk	`Get-PSDrive C | Select Used,Free`

Recent errors	`Get-WinEvent -LogName System -MaxEvents 20 | Where Level -eq 2`
Check certs	`Get-ChildItem Cert:\LocalMachine\My`
Check NIC team	`Get-NetLbfoTeam`
Failed tasks	`Get-ScheduledTask | Get-ScheduledTaskInfo | Where LastTaskResult -ne 0`

🚫 **DO NOT USE (L3 Only):**

- `Reset-ComputerMachinePassword` - Can break trust permanently
- `netdom reset` - Dangerous if misused
- `Remove-Computer` - Removes from domain
- `nltest /sc_reset` - Can cause issues

📞 When to Escalate to L3

Escalate Immediately If:

- ☐ Trust repair fails multiple times
- ☐ AD replication failures detected (on DC)
- ☐ Multiple DCs showing issues
- ☐ Cannot contact ANY domain controller
- ☐ CPU consistently >90% with no obvious cause
- ☐ SSL certificates expired for critical apps
- ☐ >50 failed logins (possible attack)
- ☐ NIC team completely down
- ☐ Security tools cannot be started
- ☐ Server cannot boot or blue screens

Information to Provide When Escalating

- ✅ Audit report (HTML/CSV from both locations)
- ✅ Steps already taken
- ✅ Error messages (screenshots)
- ✅ Server name and IP
- ✅ Time issue started
- ✅ Any recent changes