L2 Server Diagnostics Guide

Windows Server Troubleshooting for L2 Support

Version 4.0 | Author: Syed Rizvi

1. Overview

This guide provides L2 support staff with tools for diagnosing and resolving common Windows Server issues. The toolkit includes two PowerShell scripts designed to be safe and effective for L2 use.

AUDIT Script (Read-Only)

Collects diagnostic information without making any changes to the server. Creates both CSV and HTML reports with 25 comprehensive checks covering system health, security tools, services, and more.

Use this FIRST to identify issues before attempting any fixes.

FIX Script (With Prompts)

Provides 12 safe fix operations with prompts before each action. You must approve each fix individually. All actions are logged for documentation.

Use this AFTER running the audit to fix identified issues.

SAFE FOR L2: Both scripts are designed to be safe for L2 use. The audit script is completely read-only, and the fix script prompts before every action.

Report Locations: All reports automatically save to TWO locations for redundancy:

- Your Desktop folder
- C:\L2_Reports (created automatically if it does not exist)

2. How to Run the Scripts

Step-by-Step Instructions

1 Open PowerShell as Administrator

Right-click on PowerShell and select "Run as Administrator". This is required for the scripts to access system information.

2 Navigate to the script location

```
cd C:\Scripts
```

Or wherever you saved the scripts.

3 Run the AUDIT script first

```
.\L2-ServerDiagnostics-Audit-v4.ps1
```

Wait for the script to complete. It will automatically open the HTML report when finished.

4 Review the audit report

Look for any items marked as CRITICAL, WARNING, or STOPPED. These need attention.

5 Run the FIX script if needed

```
.\L2-ServerDiagnostics-Fix-v4.ps1
```

The script will prompt you before each fix. Type Y to apply or N to skip.

6 **Run the AUDIT again to verify**

After applying fixes, run the audit script again to confirm the issues are resolved.

Output Files

File	Description	Use For
L2_Audit_SERVERNAME_timestamp.csv	Comma-separated values file	Excel analysis, filtering, sorting
L2_Audit_SERVERNAME_timestamp.html	Visual HTML report	Quick review, sharing with team
L2_Fix_Log_SERVERNAME_timestamp.txt	Fix action log	Documentation of changes made

3. The 25 Checks Explained

The audit script performs 25 comprehensive checks. Here is what each check does and why it matters:

#	Check	What It Does	Why It Matters
1	System Info	Gets computer name, OS version, uptime	Basic identification and uptime tracking
2	Windows Activation	Checks if Windows is licensed	Unlicensed servers are compliance violations
3	Trust Relationship	Tests secure channel to domain	Broken trust prevents domain logins
4	Group Policy	Checks for GPO errors in last 7 days	GPO failures cause policy enforcement issues
5	AD Replication	Checks replication status (DCs only)	Replication failures affect entire domain
6	CPU Usage	Gets current CPU load percentage	High CPU causes slow performance
7	Top Processes	Lists top 5 CPU and memory consumers	Identifies resource-hungry applications
8	Memory Usage	Gets RAM usage percentage	High memory causes performance issues
9	Page File		

		Checks virtual memory usage	Full page file can cause crashes
10	Disk Space	Checks free space on all drives	Low disk causes application failures
11	Critical Services	Checks 13 essential Windows services	Stopped services cause various failures
12	NIC Teaming	Checks network adapter team status	Broken team causes network outages
13	SSL Certificates	Finds expired or expiring certs	Expired certs cause application outages
14	Security Tools	Checks Nessus, Trellix, Trend, etc.	Security tools must be running for compliance
15	Time Sync	Checks if time is synced to domain	Time drift breaks Kerberos authentication
16	Pending Reboot	Checks if server needs restart	Pending reboots can cause instability
17	RDP Status	Checks if Remote Desktop is enabled	Disabled RDP prevents remote access
18	Firewall	Checks firewall profile status	Firewall state affects connectivity
19	Scheduled Tasks	Finds failed tasks in last 7 days	Failed tasks mean missed jobs
20			

	Backup Status	Checks Windows Server Backup	Failed backups risk data loss
21	Failed Logins	Counts failed logins in last 24 hours	High count may indicate attack
22	Event Errors	Gets last 20 error events	Shows recent system problems
23	Network	Tests connectivity to DC	Network issues affect all services
24	Patches	Lists recent hotfixes	Unpatched servers are vulnerable
25	Summary	Counts critical, high, warning issues	Quick health overview

4. Security Tools Monitoring

The audit script checks for the following security tools and their status:

Tenable Nessus Agent

> **Service Name:** Tenable Nessus Agent
>
> **Installation Path:** C:\Program Files\Tenable\Nessus Agent
>
> **What We Check:**
>
> - Is the service running?
> - Is the agent linked to Tenable server?
>
> **If Not Linked:** Contact your security team for the linking key.
>
> ```
> # Check Nessus status manually cd "C:\Program
> Files\Tenable\Nessus Agent" .\nessuscli.exe agent status
> ```

Trellix (McAfee)

> **Services Checked:**
>
> - macmnsvc - Trellix Agent
> - masvc - Trellix Agent Service
> - mfefire - Trellix Firewall
> - mfemms - Trellix Management
> - McShield - Trellix Scanner
> - McAfeeFramework - Framework Service
>
> **If Stopped:** Use the FIX script to restart security services.

Trend Micro

> **Services Checked:**
>
> - ds_agent - Deep Security Agent
> - TmListen - Trend Micro Listener
> - ntrtscan - Real-Time Scan
>
> **If Stopped:** Use the FIX script to restart security services.

Other Tools

> The script also checks for:
>
> - **CrowdStrike:** CSFalconService
> - **Windows Defender:** WinDefend

5. Common Issues and How to Fix Them

Issue: Trust Relationship Broken

> **Symptoms:**
>
> - Users cannot log in with domain accounts
> - Error: "The trust relationship between this workstation and the primary domain failed"
> - Network resources inaccessible
>
> **How to Fix:**
>
> 1. Run the FIX script
> 2. Select "Repair Trust Relationship" when prompted
> 3. Enter Domain Admin credentials when asked
> 4. Run the AUDIT script again to verify
>
> **If Still Broken:** Escalate to L3

Issue: High CPU Usage

> **Symptoms:**
>
> - Server slow or unresponsive
> - CPU shows greater than 80% in audit report
> - Applications timing out
>
> **How to Investigate:**
>
> 1. Check the "Top Processes" section in the audit report
> 2. Identify which process is consuming CPU
> 3. Check if it is a known application or unexpected
> 4. Contact application team if it is their application

> **If Unknown Process:** Escalate to L3 or Security team

Issue: Low Disk Space

> **Symptoms:**
>
> - Drive shows less than 20% free in audit
> - Applications failing to write files
> - Windows updates failing
>
> **How to Fix:**
>
> 1. Run the FIX script
> 2. Select "Clean Temp Files" when prompted (if disk is low)
> 3. Check what is consuming space
> 4. Contact application team if logs are filling disk

Issue: Critical Service Stopped

> **Symptoms:**
>
> - Service shows STOPPED in audit report
> - Related functionality not working
>
> **How to Fix:**
>
> 1. Run the FIX script
> 2. The script will detect stopped services
> 3. Approve restarting each service when prompted
> 4. Run AUDIT again to verify services are running

Issue: Time Not Synced

Symptoms:

- Audit shows time source as "Local" instead of domain
- Kerberos authentication failures
- Certificate errors

How to Fix:

1. Run the FIX script
2. Select "Force Time Sync" when prompted
3. Run AUDIT again to verify time source shows domain

Issue: SSL Certificate Expiring or Expired

Symptoms:

- Audit shows certificate expiring in less than 30 days
- Application showing certificate errors

How to Handle:

1. Note the certificate name from the audit report
2. Identify which application uses it
3. Create a ticket for certificate renewal
4. Escalate to L3 or application team

Note: L2 cannot renew certificates - escalate this.

Issue: Failed Login Attempts

Symptoms:

- Audit shows high number of failed logins (greater than 20)

- User accounts getting locked out

How to Handle:

1. If less than 20: Normal, no action needed
2. If 20-50: Monitor, may be user error
3. If greater than 50: Escalate to Security team immediately

Note: High failed logins may indicate a brute force attack.

6. Safe Commands Reference

These commands are safe for L2 to run manually if needed:

Purpose	Command	What It Does
Refresh Group Policy	gpupdate /force	Reapplies all group policy settings
Check GPO Results	gpresult /r	Shows applied group policies
Sync Time	w32tm /resync /force	Forces time sync with domain
Flush DNS	Clear-DnsClientCache	Clears local DNS cache
Register DNS	ipconfig /registerdns	Re-registers DNS records
List Stopped Services	Get-Service | Where Status -eq Stopped	Shows all stopped services
Start a Service	Start-Service -Name "ServiceName"	Starts a specific service
Check CPU	Get-WmiObject Win32_Processor | Select LoadPercentage	Shows current CPU usage
Check Disk Space	Get-PSDrive C | Select Used,Free	Shows C: drive usage
View Recent Errors	Get-WinEvent -LogName System -MaxEvents 20	Shows last 20 system events

List Certificates	Get-ChildItem Cert:\LocalMachine\My	Lists installed certificates
Check NIC Team	Get-NetLbfoTeam	Shows NIC team status

7. When to Escalate to L3

Escalate to L3 if any of the following situations occur:

Escalate Immediately

- Trust relationship issues persist after running fix script
- AD replication failures detected on a Domain Controller
- Multiple Domain Controllers showing issues
- Server cannot contact ANY domain controller
- CPU consistently above 90% with no obvious cause
- SSL certificates expired for critical applications
- Greater than 50 failed login attempts in 24 hours
- NIC team completely down (network outage)
- Security tools cannot be started after multiple attempts
- Server blue screens or cannot boot
- Data corruption suspected

Information to Include When Escalating

Always provide the following when creating an L3 ticket:

- **Audit Report:** Attach both HTML and CSV from the audit
- **Fix Log:** Attach the fix script log if you ran it
- **Steps Taken:** List everything you already tried
- **Error Messages:** Include screenshots of any errors
- **Server Info:** Server name, IP address, role
- **Timeline:** When the issue started, any recent changes
- **Business Impact:** How many users affected, severity

> **Remember:** Document everything you do. The audit and fix scripts create logs automatically - always attach these to your ticket.

8. Quick Reference Card

Workflow Summary

1. Open PowerShell as Administrator
2. Run: .\L2-ServerDiagnostics-Audit-v4.ps1
3. Review the HTML report for issues
4. If issues found, run: .\L2-ServerDiagnostics-Fix-v4.ps1
5. Approve fixes by typing Y when prompted
6. Run audit again to verify fixes worked
7. If issues persist, escalate to L3 with reports attached

Status Meanings in Reports

Status	Meaning	Action Required
OK	Check passed, no issues	None
INFO	Information only	None
WARNING	Potential issue found	Review and consider fixing
CRITICAL	Serious issue found	Fix immediately or escalate
STOPPED	Service not running	Start the service
ERROR	Error event found	Review event details

Thresholds

Metric	OK	Warning	Critical

CPU Usage	Below 80%	80-90%	Above 90%
Memory Usage	Below 80%	80-90%	Above 90%
Disk Free Space	Above 20%	10-20%	Below 10%
Failed Logins (24h)	Below 20	20-50	Above 50
Days Since Patch	Below 60	60+ days	-
Cert Expiration	Above 90 days	30-90 days	Below 30 days