Secure configuration: which baseline should your servers follow, and do they still match it?

This quarter, pick one published baseline per server platform, remove default and shared credentials and switch off the legacy protocols that relay attacks need, auditing each change before you enforce it. Then apply the baseline from code to every new and existing server and compare live settings with it every week, so drift becomes a finding with an owner.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.1**

Written for

IT and platform teams running Windows and Linux servers, hypervisors, databases and other server software, on premises or on IaaS

Latest version

sheets.einblick.dev/secure-configuration/

If you only do five things

1. **Pick one baseline per platform.**
   Use Microsoft's security baseline for each Windows Server version[1], the CIS Level 1 Server profile your Linux distribution ships[20,21] and Broadcom's guide for your vSphere version[23]. Add STIG or other profiles only where a contract requires them.
2. **Remove default and shared credentials.**
   Give each Windows server its own local admin password with Windows LAPS, built into Server 2019 and later[4]. Replace default passwords on iLO, iDRAC and other management controllers[23], and don't use or enable SQL Server's `sa` login[16].
3. **Switch off what relay attacks need.**
   After an audit, require SMB signing, LDAP signing and channel binding, and remove SMBv1, NTLMv1, LLMNR and NetBIOS. Microsoft saw NTLM-related security cases rise nearly sixfold in a decade, and more in the first half of 2026 than in all of 2025[5].
4. **Lock down hypervisor management.**
   Turn on ESXi lockdown mode, which is off by default, limit the host firewall to admin networks and keep SSH stopped[23]. Mandiant advises taking hypervisors and backups out of the corporate Active Directory domain[25].
5. **Apply it from code and check for drift.**
   Keep GPOs, OSConfig settings and playbooks in version control. Google calls hardening a state to maintain against drift: UNC3944 relied on changes such as enabling SSH[24].

Roll out a baseline without breaking things

1. **Measure before you change.**
   Pick the domain controller, member server or workgroup variant for each server[3]. Compare current GPOs with it in Policy Analyzer[1], or run `oscap xccdf eval` with the profile on Linux[20].
2. **Turn on the audit events and wait.**
   Log for two to four weeks, including a month end: SMB's **Audit client does not support signing**[2], NTLM events 4020 to 4023 and 4030 to 4033[9], LSA protection events 3065 and 3066[14] and LDAP events 2889, 3074 and 3075, which need diagnostic logging and channel binding at **When supported**[11,12].
3. **Enforce in rings, with an exception list.**
   Start with IT's own servers. Give each exception an owner, a reason and an end date; BSI asks you to document and justify settings you can't apply[26].
4. **Plan the rollback before you remediate.**
   Snapshot first: Red Hat has no automated way to revert hardening[20], and removing an OSConfig baseline may not restore the old settings[3].
5. **Build new servers hardened.**
   Red Hat supports remediation only on systems in their default configuration, so install from a hardened Kickstart file or image[20]. Finish the configuration before a server reaches production or the internet[26].

Windows Server settings that matter most

- **SMB.** Remove SMBv1, which Server 2019 and later don't install[7]. Server 2025 member servers require signing only outbound[6]: audit them, then require inbound signing or EPA[2].
- **LDAP signing and channel binding.** New Active Directory deployments on Server 2025 require signing by default; channel binding defaults to **When supported** there and **Never** on 2022 and earlier[11,12]. Once the audit events stop, set **Require signing** and **Always**.
- **NTLMv1, LLMNR, NetBIOS and old TLS.** The Server 2025 OSConfig baseline allows only NTLMv2, turns off LLMNR and NetBIOS and requires TLS 1.2 or later[3]. Set the same on older servers: Server 2022 and earlier enable TLS 1.0 and 1.1 by default[13].
- **LSA protection.** Only new, domain-joined Windows 11 installs turn it on by default[14]; on Server 2025, the OSConfig baseline runs LSASS as a protected process[3]. Turn it on once the audit events are clean; with UEFI lock, as Microsoft's GPO baseline sets it, policy alone can't turn it off again[14].

Every server, Linux, databases and hypervisors

- **Unused roles and services.** Remove what a server doesn't need, including firmware functions[26]. On Windows, start with the Print Spooler on domain controllers and servers that don't print[15].
- **Linux.** RHEL 10's SCAP Security Guide has CIS, DISA STIG, PCI DSS and BSI SYS.1.1 and SYS.1.3 profiles[20]. Ubuntu's USG has CIS and STIG profiles for 20.04 to 24.04 and needs Ubuntu Pro, free only for personal use[21,22].
- **Databases.** Prefer Active Directory logins to SQL Server logins, keep `sa` disabled, leave `xp_cmdshell` off and enable only the features you use[16].
- **ESXi.** Google advises not joining hosts to Active Directory[24]; if you must, replace the default **ESX Admins** group with your own. Turn on audit records, off by default, and forward them[23]. Encrypt Tier 0 VMs[24].
- **Management controllers.** Put iLO, iDRAC and other BMCs on an isolated network with local accounts, and disable IPMI Cipher 0 and unused services[23].

What changed in 2026

- **The Windows Server 2025 baseline turned on NTLM auditing** in version 2602, published in February 2026. It says to audit SMB clients on member servers before requiring signing or EPA[2].
- **The 2011 Secure Boot certificates expired.** Servers without the 2023 certificates still boot but get no new boot-level protections[19].
- **Broadcom's 9.1 hardening guide came out in June 2026,** for VCF and vSphere Foundation 9.1, with PowerCLI audit and remediation scripts[23].
- **NTLM is going away in stages.** October 2026 updates added enhanced NTLM auditing to Server 2019 and 2022[9] and block NTLMv1-derived single sign-on by default on Server 2025[8]. Microsoft plans to disable network NTLM by default in the next major Windows Server release[10].

What you can skip

- **Every control at its strictest.** Broadcom offers a reasonable baseline, not a catalog of every control, because the strictest settings often impede daily administration[23]. Use CIS Level 1 unless a rule requires Level 2.
- **Buying CIS SecureSuite first.** Microsoft's baselines come in the Security Compliance Toolkit[1], RHEL ships CIS profiles[20] and CIS Benchmark PDFs are free for non-commercial use[28]. CIS names hosting, consulting and security products as commercial use; membership starts at $2,400 a year[27].
- **Hardening the ESXi SSH daemon.** Broadcom dropped that control: keep SSH stopped except for brief, supervised diagnostics[23].

Mistakes that cost the most

- **Enforcing signing before auditing.** Once LDAP signing is required, domain controllers reject unsigned binds and simple binds without TLS[11].
- **Two tools managing one setting.** If Group Policy and OSConfig set different values, the setting keeps flipping between them[3].
- **Weakening a whole server for one device.** Turning off SMB signing for an old NAS[7] or using RHEL's LEGACY crypto policy[20] weakens every other connection.
- **Leaving old VMs on the datastore.** UNC3944 used an orphaned VM to read a domain controller's disk[24]. Delete retired disks.

What this looks like at your size

Small team, no security staff

- Test Microsoft's baseline GPOs, or OSConfig on Server 2025, on one server per role first.
- Ask your IT provider for every default or shared password on servers, NAS, hypervisors and BMCs, and turn on Windows LAPS.
- Find the tools that log in to ESXi hosts directly, then turn on lockdown mode in vCenter.

Growing, with IT or security staff

- Keep baselines and exceptions in version control and change them by pull request.
- Run the NTLM, SMB and LDAP audits this quarter, then enforce one ring a month.
- With Defender for Servers Plan 2, check Windows servers against CIS, or STIG on Server 2019, in its baselines assessment[18].

Enterprise or regulated

- Map results to your auditors' framework: CIS, STIG, PCI DSS or BSI SYS.1.1 and SYS.1.3[29].
- Report drift with Azure Machine Configuration, free through Arc once you attest Software Assurance[17].
- Build golden images in a pipeline that fails on baseline violations.

Version history

5 Nov 2026, version 1.1 Reviewed for company readers: clarified what CIS counts as commercial use and that Ubuntu Pro is free only for personal use.

Sources

1. Microsoft Security Compliance Toolkit. Microsoft Learn, 8 Oct 2026. learn.microsoft.com
2. Security baseline for Windows Server 2025, version 2602. Microsoft Tech Community, 23 Feb 2026. techcommunity.microsoft.com
3. Deploy Windows Server 2025 security baselines with OSConfig. Microsoft Learn, 2 Jul 2026. learn.microsoft.com
4. Windows LAPS overview. Microsoft Learn, 12 Oct 2026. learn.microsoft.com
5. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
6. Control SMB signing behavior. Microsoft Learn, 15 Sep 2025. learn.microsoft.com
7. Detect, enable, and disable SMBv1, SMBv2, and SMBv3. Microsoft Learn, 8 Sep 2026. learn.microsoft.com
8. KB5066470: Manage NTLMv1 changes in Windows. Microsoft Support, updated 19 Oct 2026. support.microsoft.com
9. KB5064479: Overview of NTLM auditing enhancements. Microsoft Support, updated 13 Oct 2026. support.microsoft.com
10. Advancing Windows security: Disabling NTLM by default. Windows IT Pro Blog, 29 Jan 2026. techcommunity.microsoft.com
11. LDAP signing overview for AD DS. Microsoft Learn, 2 Oct 2026. learn.microsoft.com
12. LDAP channel binding for AD DS. Microsoft Learn, 2 Oct 2026. learn.microsoft.com
13. Protocols in TLS/SSL (Schannel SSP). Microsoft Learn, 20 Mar 2025. learn.microsoft.com
14. Configure added LSA protection. Microsoft Learn, 12 Oct 2026. learn.microsoft.com
15. Identity infrastructure security assessments. Microsoft Learn, 6 Nov 2025. learn.microsoft.com
16. SQL Server security best practices. Microsoft Learn, 19 Oct 2026. learn.microsoft.com
17. Windows Server Management enabled by Azure Arc. Microsoft Learn, 16 Jun 2026. learn.microsoft.com
18. Security baselines assessment. Microsoft Learn, 26 May 2026. learn.microsoft.com
19. KB5062710: Secure Boot certificate expiration and CA updates. Microsoft Support, updated 18 May 2026. support.microsoft.com
20. RHEL 10: Security hardening. Red Hat docs, checked 4 Nov 2026. docs.redhat.com
21. Ubuntu Security Guide (USG). Ubuntu docs, updated 22 Oct 2026. documentation.ubuntu.com
22. Ubuntu Pro pricing. Canonical, checked 5 Nov 2026. ubuntu.com
23. VCF 9.1 Security Configuration and Hardening Guide. Broadcom, 12 Jun 2026. github.com
24. Defending your VMware vSphere estate from UNC3944. Google Threat Intelligence, 23 Jul 2025. cloud.google.com
25. M-Trends 2026, Executive Edition. Mandiant, Mar 2026. services.google.com
26. IT-Grundschutz-Kompendium, SYS.1.1 Allgemeiner Server. BSI, Edition 2023. bsi.bund.de
27. CIS SecureSuite pricing for end users. CIS, checked 4 Nov 2026. cisecurity.org
28. Terms and Conditions: CIS Benchmarks (Free PDF Use). CIS, checked 4 Nov 2026. cisecurity.org