CHECKLIST

Windows Server 2022 Active Directory Hardening Checklist

A practical, vendor-neutral checklist to help reduce credential theft, lateral movement, and domain compromise while validating AD hardening changes before production rollout.

Windows Server 2022 Active Directory Hardening Checklist

Use this checklist to harden Active Directory on Windows Server 2022 without breaking core identity services, client logon, application dependencies, or recovery operations.

How to use this checklist:

- Review each item with the AD, infrastructure, security, and application owners.
- Mark each control as Done, In Progress, Not Required, or Needs Validation.
- Pilot changes in a test OU, lab domain, or a limited set of domain controllers first.
- Record rollback criteria before enabling any restriction.

---

1) Baseline and inventory

- [ ] Document all domain controllers, their OS versions, patch levels, roles, and site placement.
- [ ] Confirm consistent time synchronization across domain controllers and key identity systems.
- [ ] Inventory privileged accounts, service accounts, break-glass accounts, and delegated admin groups.

- [ ] Identify all authentication methods currently in use, including Kerberos, NTLM, LDAP signing, LDAP channel binding, and any legacy dependencies.
- [ ] Map all applications, appliances, scripts, and scheduled tasks that depend on directory authentication.
- [ ] Identify all management paths used to administer domain controllers and AD-related systems.
- [ ] Record current Group Policy Objects affecting identity, authentication, and domain controller security.
- [ ] Establish a documented rollback plan for each change set.

---

2) Privileged access and administration

- [ ] Use separate accounts for daily use and administrative access.
- [ ] Minimize permanent membership in Domain Admins, Enterprise Admins, Schema Admins, and other high-privilege groups.
- [ ] Require approval or just-in-time elevation for privileged access where possible.
- [ ] Restrict privileged logon to hardened admin workstations or approved jump hosts.
- [ ] Prevent privileged accounts from browsing email, web, or untrusted content from the same session used for administration.
- [ ] Limit who can log on interactively to domain controllers.
- [ ] Restrict local administrator rights on domain controllers to only approved personnel and systems.
- [ ] Review tiered administration or equivalent role separation for identity infrastructure.
- [ ] Ensure emergency/break-glass accounts are protected, monitored, and tested.

Validation checks:

- [ ] Confirm privileged logon is blocked from non-approved endpoints.
- [ ] Confirm admin group membership is reviewed and approved.
- [ ] Confirm break-glass account access is documented and tested.

---

3) Authentication hardening

- [ ] Prefer Kerberos for domain authentication wherever supported.
- [ ] Identify all NTLM usage and classify each occurrence as required, replaceable, or unknown.
- [ ] Restrict or phase out NTLM only after validating that critical systems do not depend on it.
- [ ] Review LDAP signing requirements and ensure clients can support them.
- [ ] Review LDAP channel binding compatibility before enforcement.
- [ ] Require strong password policy and lockout settings appropriate to your environment.
- [ ] Ensure privileged accounts use unique, strong passwords or equivalent strong authentication.
- [ ] Evaluate multi-factor authentication for administrative access and remote access paths.
- [ ] Remove or disable any authentication method that is no longer needed.

Validation checks:

- [ ] Test authentication for user logon, service logon, administration, and application access.
- [ ] Confirm no critical app still requires an authentication method slated for restriction.
- [ ] Verify lockout and password policies do not create operational issues for service accounts.

---

4) Service accounts and delegation

- [ ] Inventory all service accounts and tie each one to a specific service, application, or scheduled task.

- [ ] Remove excessive rights from service accounts that are no longer justified.
- [ ] Use the minimum privileges necessary for each service account.
- [ ] Eliminate shared service accounts where a more secure design is available.
- [ ] Review all delegation settings and document the business reason for each one.
- [ ] Remove unconstrained delegation unless there is a clearly approved exception.
- [ ] Review constrained delegation for necessity and scope.
- [ ] Confirm that service accounts do not have unnecessary membership in privileged groups.
- [ ] Rotate passwords or migrate to stronger managed identity mechanisms where supported.

Validation checks:

- [ ] Confirm each service account still functions after permission reduction.
- [ ] Verify delegated applications and integrations still authenticate and operate correctly.
- [ ] Confirm no stale or orphaned service accounts remain enabled.

---

5) Domain controller hardening

- [ ] Keep all domain controllers fully patched and on a consistent update baseline.
- [ ] Remove unnecessary software, services, and management tools from domain controllers.
- [ ] Restrict remote administration to approved management hosts.
- [ ] Limit inbound firewall exposure to only required ports and management sources.
- [ ] Disable or restrict protocols and services not required for identity operations.
- [ ] Ensure domain controllers are not used as general-purpose servers.
- [ ] Restrict file sharing, print services, and other nonessential roles on domain controllers.
- [ ] Protect administrative access with the same rigor used for other Tier 0 assets.
- [ ] Verify secure boot, virtualization-based protections, or equivalent host protections where supported and appropriate.

Validation checks:

- [ ] Confirm directory replication still works between all domain controllers.
- [ ] Confirm remote administration works only from approved sources.
- [ ] Confirm no business-critical service depends on an unnecessary DC-local component.

---

6) GPO and configuration control

- [ ] Maintain a documented security baseline for AD and domain controller settings.
- [ ] Apply changes through controlled Group Policy or change management processes.
- [ ] Avoid inconsistent manual configuration across domain controllers.
- [ ] Review and clean up obsolete GPOs, security filters, and WMI filters.
- [ ] Protect the permissions on GPOs and Group Policy links.
- [ ] Limit who can edit GPOs that affect authentication, privileged access, or domain controller security.
- [ ] Track all baseline changes with owner, date, reason, and rollback plan.

Validation checks:

- [ ] Confirm the intended GPOs are linked to the correct OUs.
- [ ] Confirm policy application is consistent across target systems.
- [ ] Confirm no conflicting GPO overrides critical hardening settings.

---

7) Auditing, logging, and alerting

- [ ] Enable auditing for changes to privileged groups.
- [ ] Enable auditing for account creation, deletion, and modification.
- [ ] Enable auditing for GPO changes.
- [ ] Enable auditing for trust changes.
- [ ] Enable auditing for directory configuration changes.

- [ ] Forward domain controller security logs to a central logging system or SIEM.
- [ ] Define alerting for high-risk events such as privileged group changes or unexpected policy modifications.
- [ ] Confirm logs are retained long enough for investigation and compliance needs.
- [ ] Test that alert routing reaches the correct responders.

Validation checks:

- [ ] Trigger a test change and confirm the event appears in logs and alerts.
- [ ] Confirm timestamps, source systems, and account names are captured clearly.
- [ ] Confirm logging survives restarts and normal maintenance windows.

---

8) Credential theft and lateral movement reduction

- [ ] Reduce standing privilege wherever possible.
- [ ] Prevent credential reuse across admin and non-admin roles.
- [ ] Protect administrative sessions from phishing and malware exposure.
- [ ] Restrict remote access paths used to reach AD management systems.
- [ ] Limit workstation-to-server trust assumptions to only what is required.
- [ ] Review local administrator password management and reuse across systems.
- [ ] Restrict lateral movement opportunities from general-purpose endpoints to identity infrastructure.
- [ ] Use network segmentation to isolate domain controllers and Tier 0 resources.

Validation checks:

- [ ] Verify an attacker on a standard workstation cannot directly reach privileged management paths.
- [ ] Verify admin credentials are not exposed on lower-trust systems.
- [ ] Verify segmentation rules do not block required identity traffic.

---

9) Recovery and resilience

- [ ] Document authoritative sources for AD recovery and restore procedures.
- [ ] Protect and test system state backups for domain controllers.
- [ ] Verify recovery credentials and procedures are available to approved personnel only.
- [ ] Confirm backup and restore processes do not rely on insecure or outdated protocols.
- [ ] Test restoration in a non-production environment when possible.
- [ ] Ensure any boot or recovery dependencies are aligned with your security design.
- [ ] If using BitLocker or similar protections, confirm recovery and network unlock procedures are validated before rollout.

Validation checks:

- [ ] Confirm a restore test can be completed successfully.
- [ ] Confirm recovery documentation is current and accessible to the right team.
- [ ] Confirm protected systems can still be recovered within operational targets.

---

10) Pilot and rollout process

- [ ] Select a small pilot group of users, servers, or domain controllers for initial hardening.
- [ ] Change one control area at a time when feasible.
- [ ] Define success criteria before applying the change.
- [ ] Define a rollback trigger for each pilot.
- [ ] Monitor authentication failures, service issues, replication errors, and admin access problems after each change.
- [ ] Expand rollout only after the pilot proves stable.
- [ ] Communicate planned changes to application, help desk, and infrastructure owners.
- [ ] Keep a change log with dates, scope, outcomes, and exceptions.

Validation checks:

- [ ] Pilot systems remain stable after the change window.
- [ ] No unexpected authentication failures are observed.
- [ ] No critical application dependencies are broken.

---

11) Final go-live review

Before moving hardening settings into production, confirm the following:

- [ ] The control is required for your risk reduction goals.
- [ ] The control was tested in a controlled environment.
- [ ] The business owner approved any known exception.
- [ ] Monitoring is in place to detect failures or abuse.
- [ ] Rollback steps are documented and understood.
- [ ] Support teams know how to validate success after deployment.

Quick pass/fail summary

Mark each as complete before rollout:

- [ ] Privileged access is separated from daily use
- [ ] Legacy authentication dependencies are identified
- [ ] Service accounts are mapped and minimized
- [ ] Delegation is reviewed and justified
- [ ] Domain controller exposure is restricted
- [ ] Logging and alerting are in place
- [ ] Backup and recovery are tested
- [ ] Pilot rollout completed without critical impact

Notes and exceptions

Use this section to record exceptions, owners, and review dates.

Item	Exception / Notes	Owner	Review Date
Privileged access			
Authentication			
Service accounts			
Delegation			
Domain controllers			
Logging			
Recovery			

Recommended next step

If your environment also allows remote administrative access to identity-related hosts, review your admin workstation and remote access posture at the same time. AD hardening is strongest when the management path is hardened with the same discipline as the directory itself.