CORVASEC

# Active Directory Troubleshooting Reference

A practical reference for domain controller health, replication, DNS, Kerberos, secure channel, Group Policy, account lockouts, and common AD DS diagnostics.

DOCUMENT CENTER

Compiled September 2026

Active Directory changes can affect authentication across an enterprise. Diagnose DNS, time, replication, and scope before forcing replication, resetting secure channels, changing SPNs, or modifying directory objects.

Use this guide as a practical reference. Verify commands, targets, permissions, paths, versions, and organizational policy before making changes. Examples with placeholders must be adapted to the environment.

# Contents


| # | Section | Entries |
|---|---|---|
| 1 | Domain controller health - first checks | 25 |
| 2 | Replication troubleshooting | 12 |
| 3 | Authentication, Kerberos, and secure channel | 15 |
| 4 | DNS and name resolution | 12 |
| 5 | Group Policy troubleshooting | 10 |
| 6 | Account, object, and lockout checks | 14 |
| 7 | Common symptom map | 6 |


Total reference entries: 94

# 1. Domain controller health - first checks

| Command | Purpose / Notes |
|---|---|
| `dcdiag /v` | Run broad domain-controller diagnostics with verbose output. |
| `dcdiag /q` | Show only errors from domain-controller diagnostics. |
| `dcdiag /test:DNS /v` | Run DNS-focused domain-controller tests. |
| `dcdiag /test:Advertising` | Verify the DC is advertising appropriate roles/services. |
| `dcdiag /test:Replications` | Check replication tests. |
| `dcdiag /test:Services` | Check required service state. |
| `dcdiag /test:SysVolCheck` | Check SYSVOL readiness. |
| `dcdiag /test:NetLogons` | Check NetLogon functionality. |
| `repadmin /replsummary` | Summarize Active Directory replication health. |
| `repadmin /showrepl` | Show inbound replication status for a domain controller. |
| `repadmin /showrepl * /csv > repl.csv` | Export replication status for review. |
| `repadmin /queue` | Show pending inbound replication requests. |
| `repadmin /showutdvec <dc> <naming-context>` | Show up-to-dateness vector information for advanced replication troubleshooting. |
| `nltest /dsgetdc:<domain>` | Locate a domain controller. |
| `nltest /dclist:<domain>` | List domain controllers for a domain. |
| `nltest /sc_verify:<domain>` | Verify the machine secure channel. |
| `nltest /dsgetsite` | Show the computer AD site. |
| `w32tm /query /status` | Show Windows Time status. |
| `w32tm /query /source` | Show the current time source. |
| `w32tm /monitor` | Monitor domain time sources. |
| `ipconfig /all` | Confirm client/DC DNS and IP configuration. |
| `nslookup -type=SRV _ldap._tcp.dc._msdcs.<domain>` | Query AD LDAP service-location records. |
| `Resolve-DnsName _kerberos._tcp.<domain> -Type SRV` | Query Kerberos SRV records with PowerShell. |
| `Get-Service NTDS,DNS,Netlogon,KDC,W32Time` | Check common AD-related service state. |
| `Get-WinEvent -LogName "Directory Service" -MaxEvents 100` | Review recent Directory Service events. |

# 2. Replication troubleshooting

| Command | Purpose / Notes |
| --- | --- |
| `repadmin /replsummary` | Identify DCs with replication failures and largest deltas. |
| `repadmin /showrepl <dc>` | Inspect partners, naming contexts, last success/failure, and error codes. |
| `repadmin /syncall <dc> /AdeP` | Trigger replication across naming contexts/partners; use after understanding the fault. |
| `repadmin /showconn <dc>` | Show connection objects. |
| `repadmin /bridgeheads` | Show bridgehead server information. |
| `repadmin /istg` | Show ISTG role information by site. |
| `repadmin /showattr <dc> "<dn>" /atts:<attribute>` | Inspect object attribute values on a specific DC. |
| `repadmin /showobjmeta <dc> "<dn>"` | Show replication metadata for an object. |
| `repadmin /showutdvec <dc> <nc> /latency` | Review up-to-dateness vector with latency data. |
| `Get-ADReplicationFailure -Scope Forest` | Show replication failures through the ActiveDirectory module. |
| `Get-ADReplicationPartnerMetadata -Target * -Scope Forest` | Review replication partner metadata. |
| `Get-ADReplicationUpToDatenessVectorTable *` | Review replication vector data where available. |

# 3. Authentication, Kerberos, and secure channel

| Command | Purpose / Notes |
|---|---|
| `klist` | Show Kerberos tickets for the current logon session. |
| `klist purge` | Purge current Kerberos tickets; affects active authentication and should be used deliberately. |
| `klist get <spn>` | Request a ticket for an SPN where supported. |
| `setspn -Q <spn>` | Search for an SPN in the forest/domain. |
| `setspn -X` | Search for duplicate SPNs. |
| `setspn -L <account>` | List SPNs registered to an account. |
| `nltest /sc_verify:<domain>` | Verify secure channel. |
| `nltest /sc_reset:<domain>` | Reset secure channel to a DC; use only after confirming the issue. |
| `Test-ComputerSecureChannel -Verbose` | Test workstation/member-server secure channel. |
| `Test-ComputerSecureChannel -Repair -Credential <cred>` | Repair secure channel using authorized credentials. |
| `Get-WinEvent -FilterHashtable @{LogName="Security";Id=4768,4769,4771}` | Review Kerberos events on a DC. |
| `Get-WinEvent -FilterHashtable @{LogName="Security";Id=4776}` | Review NTLM credential validation events. |
| `whoami /groups` | Inspect current group memberships and token. |
| `gpresult /r` | Show Resultant Set of Policy summary. |
| `gpresult /h gp.html` | Generate an HTML Group Policy results report. |

# 4. DNS and name resolution

| Command | Purpose / Notes |
| --- | --- |
| `ipconfig /all` | Verify DC/client DNS servers; domain members should normally use AD-integrated DNS as designed. |
| `ipconfig /flushdns` | Clear local DNS cache. |
| `ipconfig /registerdns` | Refresh client DNS registration. |
| `dcdiag /test:DNS /e /v` | Run enterprise-wide DNS diagnostics. |
| `nslookup <dc-fqdn>` | Resolve a domain controller hostname. |
| `nslookup -type=SRV _ldap._tcp.dc._msdcs.<domain>` | Find LDAP DC locator records. |
| `nslookup -type=SRV _kerberos._tcp.<domain>` | Find Kerberos service records. |
| `Resolve-DnsName <domain> -Type SOA` | Check domain DNS authority record. |
| `Resolve-DnsName <domain> -Type NS` | Check name servers. |
| `Get-DnsServerZone` | List DNS zones on a Windows DNS server. |
| `Get-DnsServerResourceRecord -ZoneName <zone>` | List records in a zone. |
| `Get-DnsClientServerAddress` | Review client DNS server configuration. |

# 5. Group Policy troubleshooting

| Command | Purpose / Notes |
| --- | --- |
| `gpupdate /force` | Refresh computer and user Group Policy; may prompt/reboot/logoff for some settings. |
| `gpresult /r` | Show applied policy summary. |
| `gpresult /scope computer /v` | Show verbose computer policy results. |
| `gpresult /scope user /v` | Show verbose user policy results. |
| `gpresult /h C:\Temp\gp.html` | Create a detailed HTML policy report. |
| `rsop.msc` | Open Resultant Set of Policy GUI. |
| `Get-GPO -All` | List GPOs when GroupPolicy module is available. |
| `Get-GPResultantSetOfPolicy -ReportType Html -Path .\rsop.html` | Generate PowerShell RSoP report. |
| `Get-WinEvent -LogName "Microsoft-Windows-GroupPolicy/Operational" -MaxEvents 100` | Review Group Policy operational events. |
| `nltest /dsgetsite` | Confirm correct AD site for the client. |

# 6. Account, object, and lockout checks

| Command | Purpose / Notes |
| --- | --- |
| `Get-ADUser <user> -Properties *` | Review a user object. |
| `Get-ADComputer <computer> -Properties *` | Review a computer object. |
| `Get-ADGroupMember <group> -Recursive` | Review recursive group membership. |
| `Get-ADPrincipalGroupMembership <user>` | List groups for a principal. |
| `Search-ADAccount -LockedOut` | Find locked-out accounts. |
| `Unlock-ADAccount <user>` | Unlock an account after validating the request/cause. |
| `Search-ADAccount -AccountDisabled` | Find disabled accounts. |
| `Search-ADAccount -AccountExpired` | Find expired accounts. |
| `Search-ADAccount -PasswordExpired` | Find accounts with expired passwords. |
| `Get-WinEvent -FilterHashtable @{LogName="Security";Id=4740}` | Find lockout events on domain controllers. |
| `Get-WinEvent -FilterHashtable @{LogName="Security";Id=4625}` | Review failed logons. |
| `Get-ADDomain` | Show current domain information. |
| `Get-ADForest` | Show forest information. |
| `Get-ADDomainController -Filter *` | List domain controllers. |

# 7. Common symptom map

| Symptom | Check first | Common causes |
|---|---|---|
| `Users cannot log on` | DNS, time, DC locator, 4768/4771, secure channel | DNS misconfiguration, clock skew, DC/KDC issue, account issue |
| `Replication errors` | repadmin /replsummary and /showrepl, DNS, time, RPC reachability | DNS, RPC/firewall, lingering objects, USN/metadata, site connectivity |
| `GPO not applying` | gpresult, GroupPolicy Operational log, SYSVOL/NETLOGON, DNS | Scope/filtering, replication, permissions, client processing |
| `Account locks repeatedly` | 4740, 4625, scheduled tasks/services, mobile devices | Stale credentials, services, mapped drives, apps, attacks |
| `Client finds wrong DC/site` | nltest /dsgetsite, subnets/sites, DNS SRV | Missing/misassigned AD subnet, DNS/cache, site topology |
| `Kerberos failures` | Time, SPNs, 4768/4769/4771, klist | Clock skew, duplicate/missing SPN, DNS, trust/account problems |

# Authoritative references

Use vendor and standards documentation for exact syntax, current behavior, version-specific details, licensing, and policy requirements.

### Microsoft AD DS Troubleshooting

https://learn.microsoft.com/windows-server/identity/ad-ds/manage/ad-ds-troubleshooting

### Microsoft Repadmin documentation

https://learn.microsoft.com/windows-server/administration/windows-commands/repadmin

### Microsoft Dcdiag documentation

https://learn.microsoft.com/windows-server/administration/windows-commands/dcdiag