

Of course. The Windows Domain environment has a rich set of command-line tools essential for administration, troubleshooting, and querying. Here is a comprehensive guide to the most important Windows Domain CMD commands, categorized by their function.

Important Note: Run CMD as Administrator

For most of these commands to work correctly, you must open the Command Prompt **as an administrator**. Many also require that you run them from a domain-joined machine, and some need to be run on a Domain Controller for full functionality.

Category 1: Computer & Domain Membership Commands

These commands are used to view and manage the computer's relationship with the domain.

Command	Description	Common Usage
<code>systeminfo</code>	Displays detailed configuration information about the computer and its OS.	<code>`systeminfo</code>
<code>netdom</code>	The primary command for managing domain membership.	<ul style="list-style-type: none">- <code>netdom query workstation</code> (List all domain-joined workstations)-

Command	Description	Common Usage
nltest	A powerful troubleshooting tool for domain trusts and connectivity.	<pre>netdom join %computename% /domain:MYDOMAIN /UserD:admin /PasswordD:*</pre> (Join a computer to a domain)
		-
		<pre>netdom resetpwd /s:DC01 /ud:MYDOMAIN\admin /pd:*</pre> (Reset machine account password)
		<ul style="list-style-type: none"> - nltest /dsgetdc:MYDOMAIN (List info the Domain Controller) - nltest /dclist:MYDOMAIN (List all DC domain) - nltest /server:%computename% /qu (Check if a server is a DC) - nltest /sc_verify:MYDOMAIN (Verify channel)

Category 2: User & Group Management Commands

These commands are used to manage users, groups, and group memberships.

Command	Description	Common Usage
<code>net user</code>	Manages local user accounts.	<ul style="list-style-type: none"> - <code>net user</code> (List local users) - <code>net user john /domain</code> (View domain "john" info) - <code>net group "Domain Admins" /domain</code> (List members of Domain Admins group)
<code>net group</code>	Manages global groups. (On a DC, <code>net localgroup</code> manages domain local groups).	<ul style="list-style-type: none"> - <code>net group "GroupName" UserName /add /domain</code> (Add a user to a domain group) - <code>net group "GroupName" /domain</code> (List members of a domain group)
<code>dsquery</code>	A powerful suite for querying Active Directory objects. More flexible than <code>net</code> commands.	<ul style="list-style-type: none"> - <code>dsquery user -name "John*"</code> (Find users named John*) - <code>dsquery computer -name "WS-*"</code> (Find computers starting with "WS-") - <code>dsquery group -name "Admin*"</code> (Find groups starting with "Admin")
<code>dsget</code>	Displays properties of a specific AD object. Often used with <code>dsquery</code> .	<code>dsquery user -name "john"</code>
<code>whoami</code>	Simple but crucial for identifying the current user's context.	<ul style="list-style-type: none"> - <code>whoami</code> (Current user) - <code>whoami /groups</code> (List security groups current user belongs to)

Command	Description	Common Usage
		- <code>whoami /all</code> (Show all user and privilege info)

Category 3: Network & Connectivity Commands

These commands are used to diagnose network issues related to domain services.

Command	Description	Common Usage
<code>nslookup</code>	Queries DNS, which is critical for finding Domain Controllers.	<code>nslookup _ldap._tcp.dc._msdcs.MYDOMAIN.com</code> (Find Domain Controllers via DNS SRV records)
<code>ping</code>	Tests basic network connectivity to a host.	<code>ping DC01.MYDOMAIN.com</code>
<code>telnet</code>	Tests if a specific port is open (needs to be installed first).	<code>telnet DC01 389</code> (Test LDAP port) <code>telnet DC01 445</code> (Test SMB/CIFS file share port)
<code>netstat</code>	Displays active network connections and listening ports.	<code>netstat -an</code>

Category 4: Group Policy (GPO) Commands

These commands are used to force updates and troubleshoot Group Policy application.

Command	Description	Common Usage
gpupdate	Forces an immediate update of Group Policy settings.	<ul style="list-style-type: none">- gpupdate /force (Applies all policies immediately)- gpupdate /target:computer /force (Applies only computer policies)
gpresult	Displays the Resultant Set of Policy (RSOP) for a user/computer. Extremely useful for troubleshooting.	<ul style="list-style-type: none">- gpresult /r (Summary report)- gpresult /h C:\gpreport.html (Generate a detailed HTML report)- gpresult /s COMPUTERNAME /user USERNAME /z (Very detailed output for a remote user/computer)

Category 5: Time Synchronization Commands

Time sync is critical for Kerberos authentication in a domain.

Command	Description	Common Usage
w32tm	The main tool for diagnosing and configuring the Windows Time service.	<ul style="list-style-type: none">- w32tm /query /status (Check current sync status)- w32tm /resync (Force an immediate sync)

Command	Description	Common Usage
		with the time source)
		- <code>w32tm /monitor</code> (Check time offset against domain controllers)

Practical Troubleshooting Example

Scenario: A user complains they cannot log onto their computer or access network resources.

1. **Check Basic Connectivity:** `ping DC01.MYDOMAIN.com`
2. **Check DNS Resolution:** `nslookup MYDOMAIN.com` (Should return your DC's IP)
3. **Check Secure Channel (Trust Relationship):** `nltest /sc_verify:MYDOMAIN`
 - o If this fails, you might need to reset the computer account:
`netdom resetpwd /s:DC01 /ud:MYDOMAIN\admin /pd:*`
4. **Check Group Policy (if login works but settings are wrong):** `gpresult /h C:\temp\gp.html` and review the report.

Moving to PowerShell

While CMD commands are still vital, modern Windows administration is shifting towards **PowerShell**. The Active Directory module for PowerShell (`Import-Module ActiveDirectory`) is far more powerful. Many CMD commands have direct PowerShell equivalents:

- `net user` -> `Get-ADUser`