

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
systeminfo	Displays detailed configuration information about the computer and its OS.	`systeminfo
netdom	The primary command for managing domain membership.	- netdom query workstation (List all domain joined workstations) -

Command	Description	Common Usage
nltest	A powerful troubleshooting tool for domain trusts and connectivity.	<pre data-bbox="1343 176 1769 298">netdom join %computername% /domain:MYDOMAIN /UserD:admin &gt;PasswordD:*</pre> <p data-bbox="1343 314 1747 345">(Join a computer to a domain)</p> <p data-bbox="1343 377 1365 398">-</p> <pre data-bbox="1343 414 1724 477">netdom resetpwd /s:DC01 /ud:MYDOMAIN\admin /pd:*</pre> <p data-bbox="1343 493 1792 525">(Reset machine account password)</p> <ul data-bbox="1343 599 1886 979" style="list-style-type: none"> <li>- nltest /dsgetdc:MYDOMAIN (List info the Domain Controller)</li> <li>- nltest /dclist:MYDOMAIN (List all DC domain)</li> <li>- nltest /server:%computername% /qu (Check if a server is a DC)</li> <li>- nltest /sc_verify:MYDOMAIN (Verify channel)</li> </ul>

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

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

## 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"><li>- gpupdate /force (Applies all policies immediately)</li><li>- gpupdate /target:computer /force (Applies only computer policies)</li></ul>
gpresult	Displays the Resultant Set of Policy (RSOP) for a user/computer. <b>Extremely useful for troubleshooting.</b>	<ul style="list-style-type: none"><li>- gpresult /r (Summary report)</li><li>- gpresult /h C:\gpreport.html (Get a detailed HTML report)</li><li>- gpresult /s COMPUTERNAME /user USEI /z (Very detailed output for a remote user/computer)</li></ul>

## 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"><li>- w32tm /query /status (Check current sync status)</li><li>- w32tm /resync (Force an immediate resync)</li></ul>

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`