Her sistem yöneticisine gerekli Windows işletim sistemlerinde (XP, 2003, Win7, 2008) yaygın kullanılan komut satırı araçları:

Araçlar	Ekleyen	İşlevi
Admt	Fç	Active Directory Migration Tool version 3 (ADMT v3)
Appwiz.cpl	Fç	Add /remove programs (programs and features)
appcmd	Fç	http özellikleri, web sitesini restore eder
Cmd	ka	Komut satırını çalıştır
Compmgmt.msc	ka	Bilgisayar Yöneticisi
Control userpasswords2	Ka	Gelişmiş Kullanıcı Hesabı Yönetimi
Devmgmt.msc	ka	Aygıt Yöneticisi
Diskmgmt.msc	ka	Disk Yöneticisi
Dism		Deployment Image Servicing and Management (DISM)
Dxdiag	fc	Ekran kartı hakkında bilgi
Driverquery		Kurulu aygıtları listeler. Drivequer /si -> signature listeler.
Eventcreate	Fc	Application loga olay ekler.
Fsmgmt.msc	ka	Paylaşılan Dosyalar
Gpedit.Msc	ka	GrupPolicy ayarları
Logman		Performans logu tutar.
Lusrmgr.msc	ka	Yerel Kullanıcılar ve Gruplar
Migwiz.exe		Kullanıcı ve ayarları transfer eder. Migdoc.xml ile konfigürasyon
Msconfig	fc	Boot hakkında bilgi, servisler, sürücüler, vs.
Msinfo32	ka	Sistem bilgisi
Msiexec		Windows Installer - command line. **msiexec /i A:\Example.msi**
Nbtstat		Netbios status names. C:\>nbtstat -S
Netcap	Fç	Network trafiği capture eder.
Netdiag	Fç	Network trafiğini gösterir. Hata denetimi.
Netsh	Fç	Network bileşenlerini yönetir.

		Trace loging açma dahil.
Perfmon.msc	ka	Performans Monitörü
Pnputil		Driver store
Powercfg.exe		Bilgisayarı uyku modundan çıkarmak için.
Scanstate LoadState		Veren. Profil aktarmanın birinci aşaması. Alan.
Secpol.msc	ka	Yerel Güvenlik Ayarları
Services.msc	ka	Çeşitli Servisler
syskey		Password'leri encrypt eder.
Sigverif.exe	Fç	Aygıt sürücülerinin imzalı olup olmadığını gösterir.
Slmgr.exe Slmgr.vbs		Aktivasyon ve lisans listesi. Serverı KMS host yapmak için: Slmgr.vbs /ipk
Slui.exe		Aktive etme.
Tracert	Fç	Hedefe giderken geçtiği router'ların adresi.
Winver	ka	Şu anki Windows Sürümünü Görüntüle
Wuauclt	Fç	Windows update wuauclt.exe /detectnow
W32tm.exe	FC	Saatleri eşitler (resynch)
Defrag.exe		Düzenli (her gece) olarak diski defrag eder.
Mstsc.exe		Remote desktop (terminal server client)
Wecutil		Diğer bir makineden Event viewer'ı okur
WinRM		Diğer bir makineden Event viewer'ı okur. DC'lerdeki hataları (logon failures) Windows 7 üzerinde bir liste halinde tutar.
Wsusutil		Export parametresi ile server'lar arası replicate (metadata)

Active Directory (komut satırı) araçları:

Araçlar	Ekleyen	İşlevi
Adsiedit	fc	PSO nesnesi. Şema düzenleme.
LDIFDE	fc	Active directory nesnelerini import, export eder ayrıca değiştirir. dn: CN=faruk,CN=Users,DC=fcholding,DC=com changetype: delete
CSVDE	fç	Active directory nesnelerini import, export eder
NTDSUTIL	fç	
DCDIAG	fç	DCDiag.exe ne yapar? Bu komut satırı aracı bir domaindeki etki alanı denetleyicilerinden (Domain COntroller) birinin veya tümünün durumunu çözümler ve sorunun giderilmesine yardımcı olmak üzere sorunları raporlar.
Dsmgmt		RODC yönetir.
Share and Storage Management		ABE-access based enumeration
Dfsdiag		DFS replikte etmiş mi?
Movetree.exe		move Active Directory objects such as contacts between domains in a single forest. Operations such as these are performed to support domain consolidation or organizational restructuring operations.
Admt	Fç	The Active Directory Migration Tool version 3 (ADMT v3) simplifies the process of restructuring your operating environment to meet the needs of your organization. You can use ADMT v3 to migrate users, groups, and computers from Microsoft® Windows NT® 4.0 domains to Active Directory® directory service domains; between Active Directory domains in different forests (interforest migration); and between Active Directory domains in the same forest (intraforest migration). ADMT v3 also performs security translation from Windows NT 4.0 domains to Active Directory domains and between Active Directory domains in different forests.
Repadmin		Replikasyonu gösteriyor. Replikasyonu yapıyor. Repadmin /showrepl Repadmin /replsummary
Dsacls		access control lists (ACLs) yönetir.
Netdom		İsim veriyor. Trust yaratır.

Dcgpofix.exe /target:dc		Restore default domain controller policy
Dsdbutil		AD LDS snapshot'unu mount eder.
Ldp.exe		Ldp.exe, arama ölçütü verilen özel bilgiler için Active Directory Basit Dizin Erişim Protokolü (LDAP) – (directory sistemleri için) aramaları destekler. .
Netlogon		Oturum açma ve srv kaydı güncelleme. …

Network Servisleri (DNS, DHCP gibi) (komut satırı) araçları:

Araçlar	Ekleyen	İşlevi
DNSCMD	fc	DNS yönetimi
PING PATHPING		TCP /IP protokolü – adresin kontrolü
TRACERT		TCP /IP protokolü – adresin ve route'ın kontrolü
ARP		Arp IP adresleri ve IP adreslerinin çözümlenmiş adreslerini gösterir.
IPCONFIG		IP konfigürasyonunu verir. / Release, Renew Flushdns Registerdns Displaydns
NBTSTAT		Mevcut TCP/IP bağlantılarını ve protokol istatistiklerini NBT (Net Bios Over TCP/IP) kullanarak gösterir. NBTSTAT –R "R" parametresi ile cache temizler.(purge)
NETSTAT		Komut satırında yürütülen "netstat" komutu etkin TCP bağlantılarını gösterir. NETSTAT -r
Netsh		Lokal ya da uzak bilgisayarların ağ bileşenleri için komut dosyası oluşturmaya yarayan ve komut satırından çalışan bir programdır. Network bileşenlerinin konfigürasyonunda da kullanılır.
NSLOOKUP		Domain adı ya da NS'ın IP adresini verir.
Netdiag		DNS kaydını değerlendirmek için kullanılır.
Jetpack.exe		DHCP database bakım.

Güvenlik (komut satırı) araçları:

Araçlar	Ekleyen	İşlevi
Cipher.exe	fç	şifreleme
Secedit.exe Security Configuration Wizard		Güvenlik Şablonlarını yönetir.
certutil		Autoenrol. Sertifika Keylerin yedeklerini alır. Certutil.exe –clr Sertifikasını revoke edilmiş. Fc-Web sitesine erişimi engeller.
MBSA		Bilgisayarın açıklarını listeler.
Lcacls.exe		ACL (izinler) görmeyi ve düzenlemeyi sağlar. N- none C- Change/Write F- Full R- Read
SetACL.exe:		ACL'leri izinler düzenler.
Wecutil		Security logları üzerinde fc ayarları.
Get-ADUser		Last logon time'ı gösterir. Text dosya olarak liste çıkarır bir parametre ile.
Nmcap		Network capture Minimum cpu kullanarak
Netmon		Network capture

PowerShell

Test-AppLockerPolicy

Enable-ADOptionalFeature Active Directory REcycle bin'i enable eder.

Önemli Portlar

Network protokolleriyle ilgili konularda yaygın kullanılan TCP/IP protokolleri ve port numaraları (TCP/UDP):

CHARGEN	TCP: 19
DHCP	UDP: 67
DNS	UDP: 53
ECHO	UDP: 7
ESP ve AH – IPSEC	TCP: 50 51
FTP	TCP: 21
FTP-DATA	TCP: 20
HTTP	TCP: 80
HTTPS	TCP: 443
IMAP4	TCP: 143
Kerberos Admin	TCP: 749
Kerberos	TCP: 88
LDAP	TCP: 389
LDAP SSL	TCP: 636
L2TP	TCP: 1701
POP3	TCP: 110
PPTP	TCP: 1723
RADIUS	TCP: 1812
RDP	TCP: 3389
SMTP	TCP: 25
SNMP	UDP: 161, 162
SSH	TCP: 22
TACACS	TCP: 49
TELNET	TCP: 23
TFTP	UDP: 69
VPN	TCP: 1723, 1701 (L2TP) GRE 47

SMB	TCP 445
END POINT MAPPER	TCP 135
NETBIOS	TCP 139
SQL SERVER	1433
Tftp	udp 69