Netstat

Beschreibung: Mit diesen Statistiken kann man herausfinden, welche Ports geöffnet sind oder welche Verbindungen zu entfernten Rechnern bestehen. Für bestehende Verbindungen lässt sich unter anderem die Adresse der Gegenstelle ablesen.

Netstat -a: Displays all connections and listening ports.

Netstat -e: Displays Ethernet statistics

Netstat -r: Displays the contents of the routing table

Arp

Beschreibung: Das Address Resolution Protocol (ARP) ist ein Netzwerkprotokoll, das zu einer Netzwerkadresse der Internetschicht die physische Adresse (Hardwareadresse) der Netzzugangsschicht ermittelt und diese Zuordnung gegebenenfalls in den so genannten ARP-Tabellen der beteiligten Rechner hinterlegt.

arp -d: Removes the listed entry from the ARP cache

arp -s: Adds a static entry to the ARP cache

arp -a: Displays all the current ARP entries for all interfaces

Ping

Beschreibung: Unter dem Ping-Wert versteht man die Zeitspanne zwischen dem Aussenden eines Datenpaketes an einen Empfänger und des daraufhin unmittelbar zurückgeschickten Antwortpaketes.

Ping (cont)

Ping -t: Pings the specified host until stopped. To see statistics and continue type Control-Break. To stop type Control-C.

Ping -l: Sends packets of a particular size.

Ping -r: Records the route for count hops.

Tracert

Beschreibung: Trace Route (traceroute / tracert) Trace Route ist ein Kommandozeilen-Tool, um in einem IP-Netzwerk den Weg von Datenpaketen zu verfolgen und sichtbar zu machen. Es geht darum festzustellen, welche Stationen ein Datenpaket bis zum Ziel nimmt.

Tracert -d: This option prevents tracert from resolving IP addresses to hostnames, often resulting in much faster results.

Tracert -h: This tracert option specifies the maximum number of hops in the search for the target. If you do not specify MaxHops, and a target has not been found by 30 hops, tracert will stop looking.

Tracert -6: This option forces tracert to use IPv6 only.

Nslookup

Beschreibung: Den Host-Namen eingeben kann und dann dessen dazugehörige IP-Adresse erhält. Ein sogenannter Reverse Lookup ist ebenfalls möglich, um den Host-Namen zu einer bestimmten IP-Adresse zu finden.

Nslookup (cont)

nslookup (ENTER) dann domainname.xy: gibt die grundlegenden Ergebnisse aus

set q=any (ENTER) - legt fest, dass so viele Ergebnisse wie möglich angezeigt werden

set q=mx (ENTER) - legt fest, dass alle Einstellungen für Mail angezeigt werden.

MBSA

Beschreibung: MBSA (Microsoft Baseline Security Analyzer) ist ein kostenloses Werkzeug, das Windows auf Sicherheitslücken untersucht. Es soll etwa typische sicherheitsrelevante Fehlkonfigurationen in Microsoft-Produkten und Windows ausfindig machen. Außerdem überprüft es, ob alle aktuellen Sicherheitsupdates vorhanden sind. Das Programm kann ohne Gültigkeitsprüfung bei Microsoft heruntergeladen werden

-qp: This switch instructs MBSA to not show scan progress.

-u: This switch lets you specify the user name of an administrator-level user on the target computer(s).

-nd: This switch instructs MBSA to not download any files from the Microsoft Web site when performing a scan. In other words, it instructs MBSA to perform the scan like it would in offline mode.

Nirsoft wnetwatcher

Beschreibung: Wireless Network Watcher is a small utility that scans your wireless network and displays the list of all computers and devices that are currently connected to your network.

/cfg <Filename>: Start Wireless Network Watcher with the specified configuration file. For example: WNetWatcher.exe /cfg "c:\config\wnw.cfg" WNetWatcher.exe /cfg "%AppData%\WNetWatcher.cfg"

/stext <Filename>: Scan your network, and save the network devices list into a regular text file.

/shtml <Filename>: Scan your network, and save the network devices list into HTML file (Horizontal).

ipconfig

Beschreibung: ipconfig ist ein Befehl des Betriebssystems Microsoft Windows die Hardwareadressen bzw. die IP-Adressen der im lokalen Netzwerk verwendeten Geräte anzeigt.

ipconfig -all: Show detailed information

ipconfig -renew: renew all adapters

ipconfig -flushdns: Clears the contents of the DNS resolver cache.

Windows Performance Analyzer

Beschreibung: WPA is a powerful analysis tool that combines a very flexible UI with extensive graphing capabilities and data tables that can be pivoted and that have full text search capabilities. WPA provides an Issues window to explore the root cause of any identified.

Windows Performance Analyzer (cont)

CTRL+O: Open a new trace or session

CTRL+G: Show and navigate to Graph Explorer

F1: Open WPA help site

MXToolbox

Beschreibung: This website can do Tests on every domain to test, if the are legit etc..

Blacklist: The blacklist check will test a mail server IP address against over 100 DNS based email blacklists

SMTP Diagnostics: This test will connect to a mail server via SMTP, perform a simple Open Relay Test and verify the server has a reverse DNS (PTR) record.

Domain Health: The Domain Health Check will execute hundreds of domain/email/network performance tests to make sure all of your systems are online and performing optimally

Pathping

Beschreibung: Pathping ist ein erweiterter Windows-Befehl zu Tracert und Ping. Im Gegensatz zu Tracert liefert Pathping detaillierte Informationen über die Weiterleitung der Pakete zu den einzelnen Rechnern

PathPing -n: Does not resolve addresses to host names.

Pathping -p: Number of milliseconds to wait between pings.

Pathping (cont)

Pathping -T: Attaches a layer 2 priority tag to the packets and sends it to each of the network devices in the path. This helps in identifying the network devices that do not have layer 2 priority configured properly. The -T switch is used to test for Quality of Service (QoS) connectivity.

Tcpview

Beschreibung: TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections.

Using Tcpvcon: *Tcpvcon usage is similar to that of the built-in Windows netstat utility:*

-a: Show all endpoints (default is to show established TCP connections).

-n: Don't resolve addresses.

Sysinternals Process Explorer

Beschreibung: Process Explorer shows you information about which handles and DLLs processes have opened or loaded.

-l: Dump the sizes of pagefile-backed sections.

-r: Flag DLLs that relocated because they are not loaded at their base address.

-t: Show process tree.

Route

Beschreibung: Eine Routingtabelle (auch Routing Information Base) enthält Angaben zu möglichen Wegen, zum „optimalen“ Weg, zum Status, zur Metrik, d. h. dem Bewertungsmaßstab des Weges, und zum Alter. Grundlage ist die Verknüpfung der Ziel-IP-Adresse mit einer Richtungsangabe in Form des Folgerouters und des Interfaces, über den der Paketstrom zu lenken ist.

Route -f: Clears the routing table of all gateway entries. If this is used in conjunction with one of the other commands, the tables are cleared prior to running the command.

Route -Print < destination >: Prints a route to the specified host. Optionally, prints the routes for the specified destination.

Route -Change <destination> Mask <netmask> <gateway> Metric <metric> if <interface>: Modifies an existing route.

Windows Performance Toolkit

Beschreibung: The Windows Performance Toolkit consists of two independent tools: Windows Performance Recorder (WPR) and Windows Performance Analyzer (WPA). In addition, support is maintained for the previous command-line tool, Xperf. However, Xperfview is no longer supported. All recordings must be opened and analyzed by using WPA.

IControlErrorInfo: Provides functions that obtain information about errors that occur when the control manager performs an operation.

Windows Performance Toolkit (cont)

IOnOffTransitionManager: Enables the client to store the profiles of the IProfileCollection to the registry for boot tracing.

IProfile: Represents an individual profile that the client controls.

Microsoft Assessment and Planning Toolkit

Beschreibung: The Microsoft Assessment and Planning Toolkit makes it easy to assess your current IT infrastructure for a variety of technology migration projects. This Solution Accelerator provides a powerful inventory, assessment, and reporting tool to simplify the migration planning process.

How to run MAP tool: - Open MAP tool - Create inventory database which will be used to save inventory data and collected statistics inside it when working with the MAP tool , by default SQL express is installed by default when installing MAP tool , SQL express is used to host the inventory database. - After creating the database. the MAP console launches giving the option to select your Inventory scenario , since MAP tool can be used to target different scenarios like SQL database consolidation, VM migration, windows upgrade, lync readiness check, etc…