**Netyard - Trainingstag**

Netzwerkdrucker:

Fileserver

Printmanagement:

* Erster Schritt (unter Printserver -> FS (local) -> Drivers) immer **Treiber** installieren. Den Treiber, der vom Hersteller empfohlen wird, direkt von der Website. PCL (Standard) und Poststrip (Grafik eher).
* **Port**: Einen Drucker über einen IP-Port einrichten. Dhcp verteilt automatisch IP-adressen (IPv4 wichtig), Leasetime = 8 Tage (Oder weniger) Lease = ändert deine IP, wenn du willst.
* **Netzwerk (IPv4)** Klasse A: ersten Drei Ziffern fest, Klasse B: ersten 6 Ziffern fest, Klasse C: ersten 9 Ziffern fest. Private Netze: C: 192.168.xxx.0/24 (Subnetzmaske: 255.255.255.0 (letzte 0 = letzte Ziffer der IP). Die vorletzten 3 Ziffern Firma und letzten 3 Privat. Private Bereich hat auch ein Klasse B Netz: 172.16(-31).0.0/16 (Subnetzmaske: 255.255.0.0. Server: 172.16.1.000, Clients: 172.1.2.000, usw. Klasse A: 10.10.0.0/8 (Subnetzmaske: 255.0.0.0). (Supernetting) Netzwerkadressen ausrechnen.
* **Reservations:** Feste IP - Mac-Adresse (eindeutige Kennung-ändert sich nicht) und schreibe darauf eine IP Adresse fest.
* Der Drucker ist über die IP immer erreichbar. Wenn ich die IP im Browser eingebe, komme ich auf den Drucker drauf.
* **Printers:** Welche Drucker hinterlegt sind, also eingerichtet. Type 3 Standard (Microsoft selbst hat Type 4)
* **Set Printing Default**: Standard-Einstellungen des Druckers
* Druckerverteilung = Zeitaufwendig zu viele Verteilungen bringen Fehler. (2-3 sind ok).
* Einstellungen: Sharing, Haken bei List in directory, sonst sieht man den Drucker nicht, in seinem Netzwerk.
* **QDS Abfragen**: Printers nach QDS. „Printers.qds“ -> ausführen = Find Printers. Kann man alle Drucker finden.

Gruppenrechtlinien:

* **Group Policy Management**
* Group Policy Objects -> Deploy\_Printers
* Loopback Processing mode (merken)
* MSI Paket kann nur ausgerollt werden.
* ADMX Dateien sind Gruppenrechtlinien
* Gp update / force (aktuelle Gruppenrechtlinien vom Domaincontroller ziehen)

Verteilung der Drucker mit Gruppenrechtlinien:

* GPP Group Policy Preferences
* Item Level Targeting: User
* Printer Properties: General: Update bei Action
* Printer Properties: Common: Rin in logged –on user’s …+ Item Level Targeting (ohne Item Level Targeting wird der für alle angewendet)
* Targeting Editor: Auf den User bezogen. SID bestimmt den User. SID= ID des Users im AD (bleibt)

CMD Befehle:

* „gpupdate /force“: Datet Veränderungen vom AD DS ab
* „gpresult /r“: Zeigt an ob Gruppenrechtlinien auch angewendet werden. Benutzerbezogen (Zugriffbezogen)
* „gpresult /r /scope:computer“: Zeigt alle Rechtlinien Computerbezogen (Geht nur, wenn man das als Administrator ausführt)
* „gpresult /z“: Zeigt Zusatzinfos (eher irritierend)
* „gpresult/ r >c:\(*Pfad, wo es abgespeichert werden soll*)\gpresult.txt“: Dann erstellt er dir eine Datei mit den Infos
* „gpresult /h c:\(*Pfad, wo es abgespeichert werden soll*)\gpresult.html“: Erstellt dir eine HTML Datei (schöner aber unübersichtlicher)
* „gpresult /x c:\(*Pfad, wo es abgespeichert werden soll*)\gpresult.xml“: Erstellt dir eine xml Datei

Gruppe erstellen:

* AD Users and Computers
* Neues OU erstellen
* Neue Gruppe erstellen

Virtualisierung:

* Hyper V
* VM Ware

Switchen und VLAN:

* Switchserverschrank
* VLan1 ist immer Standard
* Untak port / Sauberer
* Tak port (intiligente)
* Ein Switch kann mehrere VLans (eigene Virtuelle Netzwerke haben) So können diejenigen die im VLan 1 sind nicht in das Netzwerk von denen, die im VLan 2 sind.
* Trunk-Port
* Mit **VLAN**-**Trunking** lassen sich Switches so verschalten, dass sie mehrere verschiedene **VLANs** untereinander zu Netzwerken verbinden. **VLAN**-**Trunking** ist in der Lage, die Informationen mehrerer virtueller LANs über eine einzige Leitung zu übertragen.
* Access-Ports, General-Ports, Trunk-Ports, Other-Ports

Firewalls:

* Sicherungssystem, das ein Netzwerk oder einen einzelnen Computer vor unerwünschtem Zugriff über Datenleitungen von außen, besonders über das Internet, schützt
* Proxy actions – Domain Names Rules

Googlen:

* Obde (out of the Box Experience)-System Prep. (Generalisierung)
* Veeam (Backup)
* Arp – a. Jedes Netzwerk hat eine Arpliste. Arp table
* Edit Dynamic Address Table -> Dort sieht man welche Mac-Adressen wirklich genutzt werden
* VLAN
* Enterprise Version 2022.2.20.0 64 bit
* Virenschutz – wichtig – Panda adapted devence
* Threat map firewall
* Powershell – Virus finden?
* 2 faktor Autorisierung