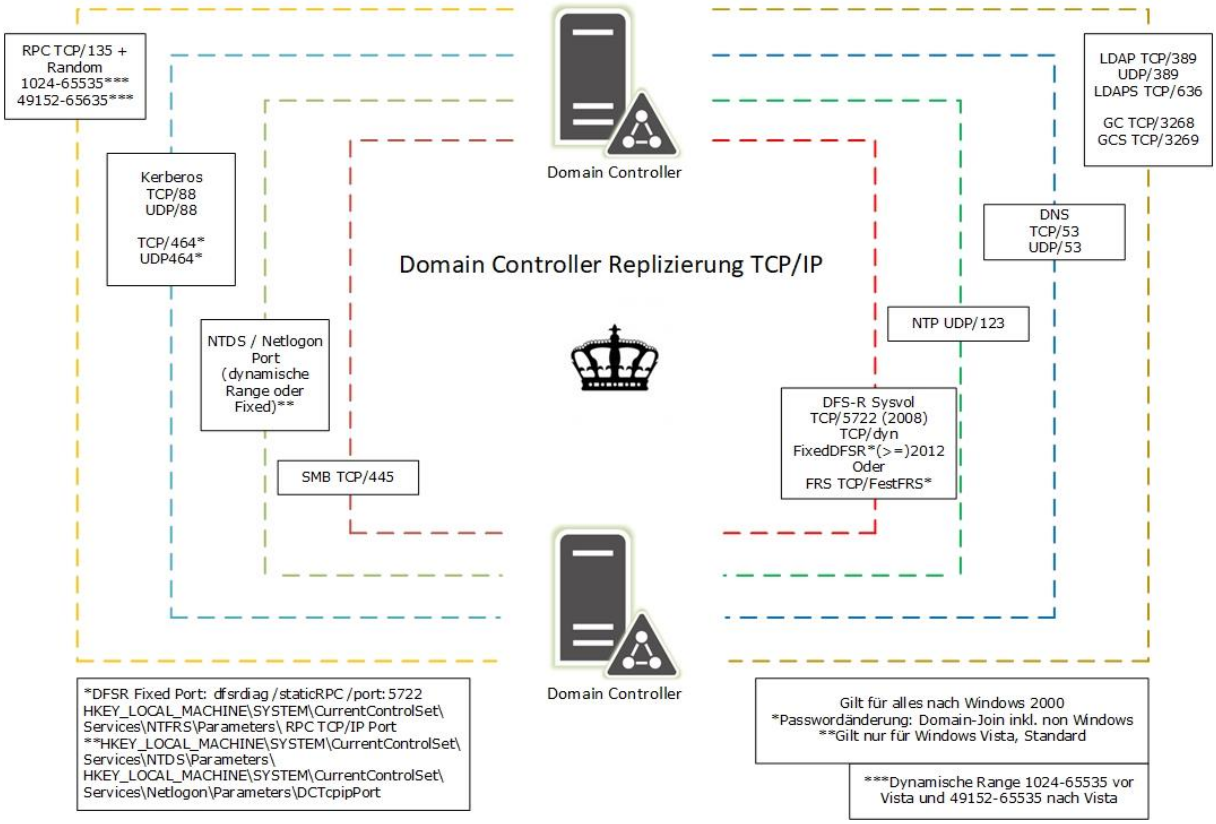
AD Ports & Services

In diesem Dokument beschreibe ich die mir bekannten und wichtigen Ports für einen sicheren Betrieb des Active Directorys.



TCP und UDP 389	LDAP	
TCP 636	LDAP SSL	
TCP 3268	GC	
TCP und UDP 88	Kerberos	
TCP und UDP 53	DNS	
TCP und UDP 445	SMB über IP	
TCP 25	SMTP	
TCP 135	dynamisch	RPC, ECM

Ports für Vertrauenstellungen

Clientport	Serverport	Art des Datenverkehrs
UDP 137	UDP 137	NetBIOS-Namensauflösung
UDP 138	UDP 138	NetBIOS-Datagrammdienst
TCP dynamisch	TCP 139	NetBIOS-Sitzungsdienst

Erstellt von Jörn Walter **24.06.2018**

AD Ports & Services

Gemischte Umgebungen

Clientport	Serverport	Art des Datenverkehrs
TCP dynamisch	TCP 135, 49152–65535	RPC, EPM
TCP und UDP dynamisch	TCP und UDP 389	LDAP
TCP dynamisch	TCP 636	LDAP SSL
TCP dynamisch	TCP 3268	GC
TCP dynamisch	TCP 3269	GC SSL
TCP und UDP 53 dynamisch	TCP und UDP 53	DNS
TCP und UDP dynamisch	TCP und UDP 88	Kerberos
TCP und UDP dynamisch	TCP-NP und UDP-NP 445	Sicherheitskontenverwaltung (Security Accounts Manager, SAM), LSA
TCP dynamisch	UDP 138	NetBIOS-Datagrammdienst

Globaler Katalog

Port	Art des Datenverkehrs
TCP 3268	GC
TCP 3269	GC SSL

Schreibgeschützte Domänencontroller

Port	Art des Datenverkehrs
TCP 3268	GC
TCP 3269	GC SSL

RODC in einem Umkreisnetzwerk mit einem schreibbaren Domänencontroller

Port	Art des Datenverkehrs
TCP 57344	DRSUAPI, LsaRpc, NeLogonR
TCP statisch 53248	FRsRpc
TCP und UDP 389	LDAP
TCP 3268	GC
TCP 445	DFS, LsaRpc, NbtSS, NetLogonR, SamR, SMB, SrvSvc
TCP und UDP 53	DNS
TCP 88	Kerberos
UDP 123	Windows-Zeitdienst (W32time)

Erstellt von Jörn Walter **24.06.2018**

AD Ports & Services

TCP und UDP 464	Kerberos-Kennwort ändern/festlegen

Mitgliedsserver in einem Umkreisnetzwerk mit einem RODC

Port	Art des Datenverkehrs
TCP 135	RPC, EPM
TCP und UDP 389	LDAP
TCP 445	DFS, LsaRpc, NbtSS, NetLogonR, SamR, SMB, SrvSvc
UDP 53	DNS
TCP 88	Kerberos
TCP und UDP 464	Kerberos-Kennwort ändern/festlegen
TCP dynamisch	DNS, DRSUAPI, NetLogonR, SamR

DNS

Port	Art des Datenverkehrs
TCP und UDP 53	DNS

DHCP

Port	Art des Datenverkehrs
UDP 67	DHCP
UDP 2535	MADCAP

WINS

Port	Art des Datenverkehrs
TCP und UDP 42	WINS-Replikation
UDP 137	NetBIOS-Namensauflösung

Benutzer- oder Computerauthentifizierung

Port	Art des Datenverkehrs
TCP und UDP 445	SMB/CIFS/SMB2
TCP und UDP 88	Kerberos
UDP 389	LDAP
TCP und UDP 53	DNS
TCP dynamisch	RPC

Erstellt von Jörn Walter **24.06.2018**

AD Ports & Services

Gruppenrichtlinien

Port	Art des Datenverkehrs
TCP und UDP dynamisch	DCOM, RPC, EPM
TCP 389	LDAP
TCP 445	SMB

Active Directory-Webdienste

Port	Art des Datenverkehrs
TCP 9389	SOAP

Anwendungsfall Remote-Management

LDAP 389,636

Kerberos 464

TCP SMB 445

TCP_UDP NetBios,NBT 137

TCP_UDP RPC,DCOM,WMI 135,593 & 1023+

TCP_UDP ICMP Port 7

TCP WinRM 5985,5986

TCP RDP 3389

TCP Dynamic RPC 49152-65535

HTTPS 443

SNMP 161,162

AD Ports & Services

RPC High Ports regeln:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Internet]
"Ports"=hex(7):34,00,33,00,30,00,30,00,30,00,2d,00,34,00,33,00,39,00,39,00,39,\

  00,00,00,00,00
"PortsInternetAvailable"="Y"
"UseInternetPorts"="Y"
```

Direkt in die Registry setzen:

```
reg add HKLM\SOFTWARE\Microsoft\Rpc\Internet /v Ports /t REG_MULTI_SZ /f /d 43000-43999

reg add HKLM\SOFTWARE\Microsoft\Rpc\Internet /v PortsInternetAvailable /t REG_SZ /f /d Y

reg add HKLM\SOFTWARE\Microsoft\Rpc\Internet /v UseInternetPorts /t REG_SZ /f /d Y
```

Der Wert Y = bestätigt und übernimmt die zuvor angegebene Port Range

PIA = PortsInternetAvailable Key value
UIP = UseInternetPorts Key value

The value of the Ports key, for sake of this example, is 5000-5100 for each entry.

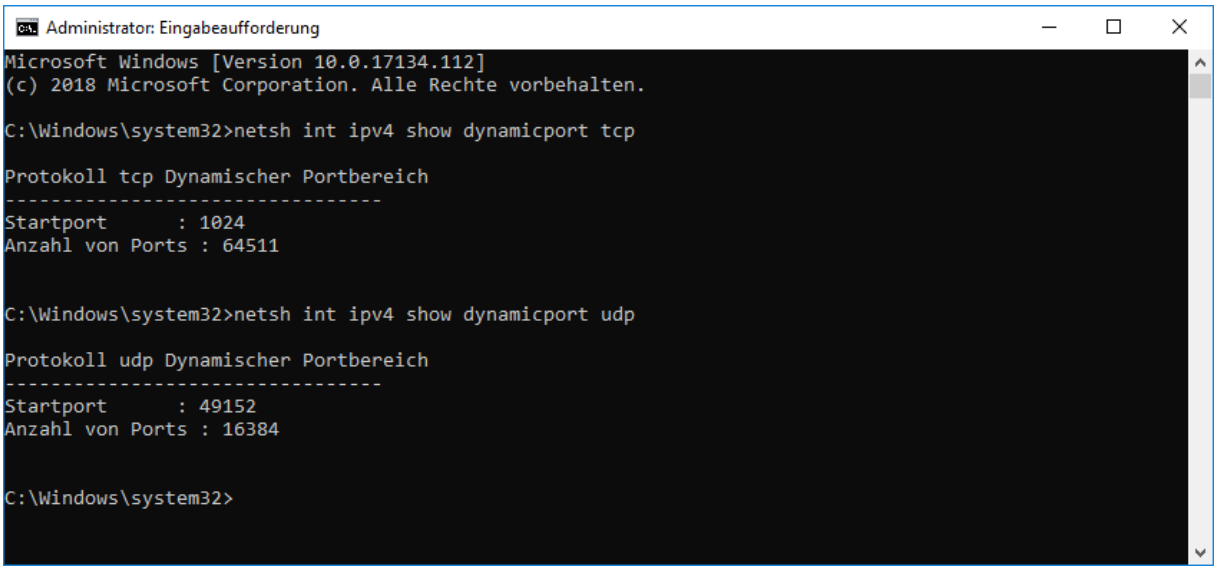
Application	PIA	UIP	Result
InternetApp	Y	Y	Uses ports between 5000 and 5100
LocalApp	Y	Y	Uses a port outside the 5000-5100 range
DefaultApp	Y	Y	Uses ports between 5000 and 5100
InternetApp	Y	N	Uses ports between 5000 and 5100
LocalApp	Y	N	Uses a port outside the 5000-5100 range
DefaultApp	Y	N	Uses a port outside the 5000-5100 range
InternetApp	N	Y	Uses a port outside the 5000-5100 range
LocalApp	N	Y	Uses ports between 5000 and 5100

AD Ports & Services

DefaultApp	N	Y	Uses a port outside the 5000-5100 range
InternetApp	N	N	Uses a port outside the 5000-5100 range
LocalApp	N	N	Uses ports between 5000 and 5100
DefaultApp	N	N	Uses ports between 5000 and 5100

Verfügbare Ports auslesen:

netsh int ipv4 show dynamicport tcp
netsh int ipv4 show dynamicport udp
netsh int ipv6 show dynamicport tcp
netsh int ipv6 show dynamicport udp



Port Range setzen:

netsh int ipv4 set dynamicport tcp start=43000 num=1000
netsh int ipv4 set dynamicport udp start=43000 num=1000
netsh int ipv6 set dynamicport tcp start=43000 num=1000
netsh int ipv6 set dynamicport udp start=43000 num=1000