LLMNR - DNS WINS NetBIOS

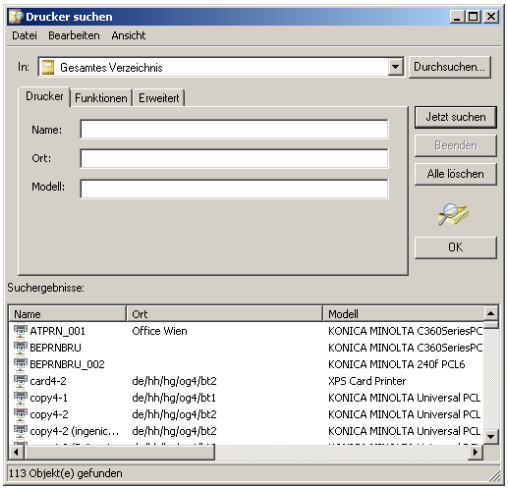
Zur Auflösung von Hostnamen in IP-Adressen und umgekehrt gibt es ein Vielzahl von Techniken und Protokollen.

DNS ist die Technik zum Auflösen von IP-Adressen, gefolgt von weiteren:

LLMNR um das es aktuell geht, ist quasi eine zweite DNS Ebene und verfügt über einen eigenen Resolver-Cache, löst auch nur lokale (Subnetz) IP-Adressen auf, die über DNS nicht aufgelöst werden können oder DNS nicht vorhanden ist.

NetBIOS-Namen werden mithilfe des WINS-Dienstes in IP-Adressen aufgelöst. WINS nutzt NetBIOS über TCP/IP und ist ein unverzichtbares Werkzeug zur Namensauflösung und wichtig für Anwendungen die mit Browser-Listen arbeiten.

Hier ein Beispiel wie ein Browser-Listening aussehen könnte:



Sollte es keinen WINS im Netzwerk geben, dann werden die NetBIOS Namen über Broadcast aufgelöst, was aber wiederum den Netzwerkverkehr und das Grundrauschen erhöht.

Okay, jetzt könnte man argumentieren und sagen; wir haben viele kleine Netzte, stört uns nicht, aber die Active-Directory- und Server- Verantwortlichen werden das anders sehen. Zur vollständigen und sauberen Namensauflösung gehört WINS/NetBIOS und DNS ins Netzwerk wie der Hypervisor zur Virtualisierung.

Welche Ports werden wofür benutzt?

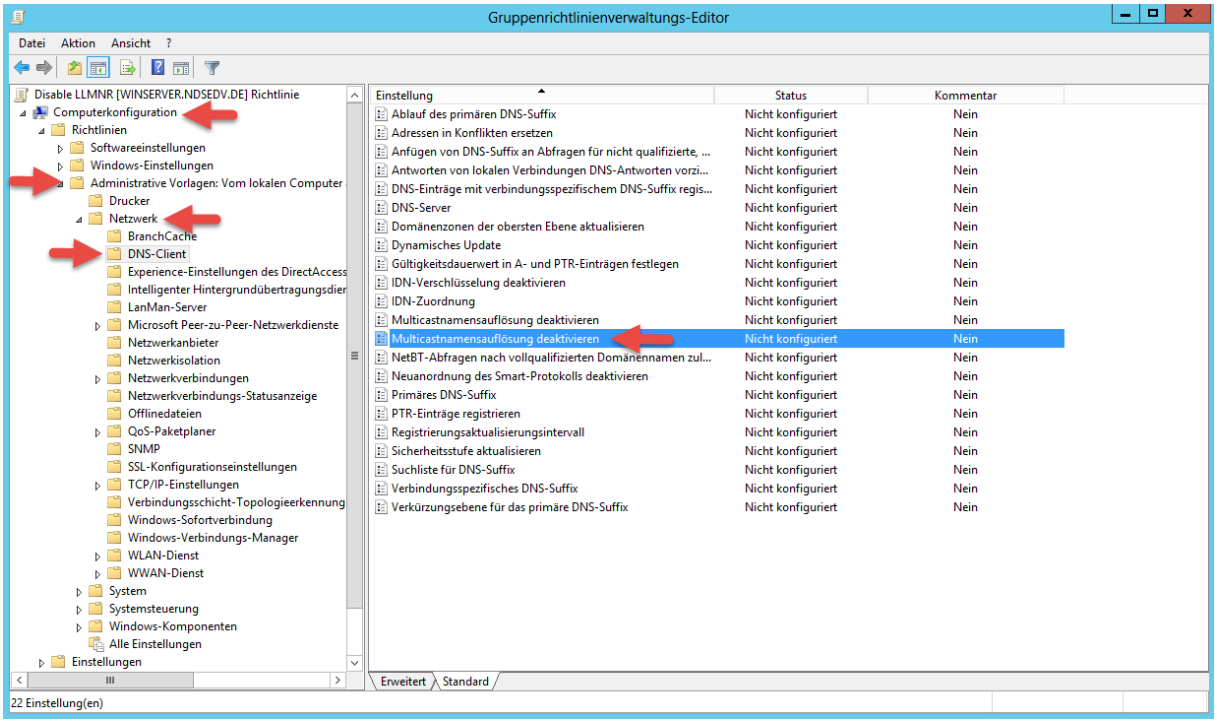
DNS Port 53
WINS Port 137, 138, 139 und 445
NetBIOS UDP 137, 138, 139
LLMNR Multicast 5353; Unicast 5355

LLMNR - DNS WINS NetBIOS

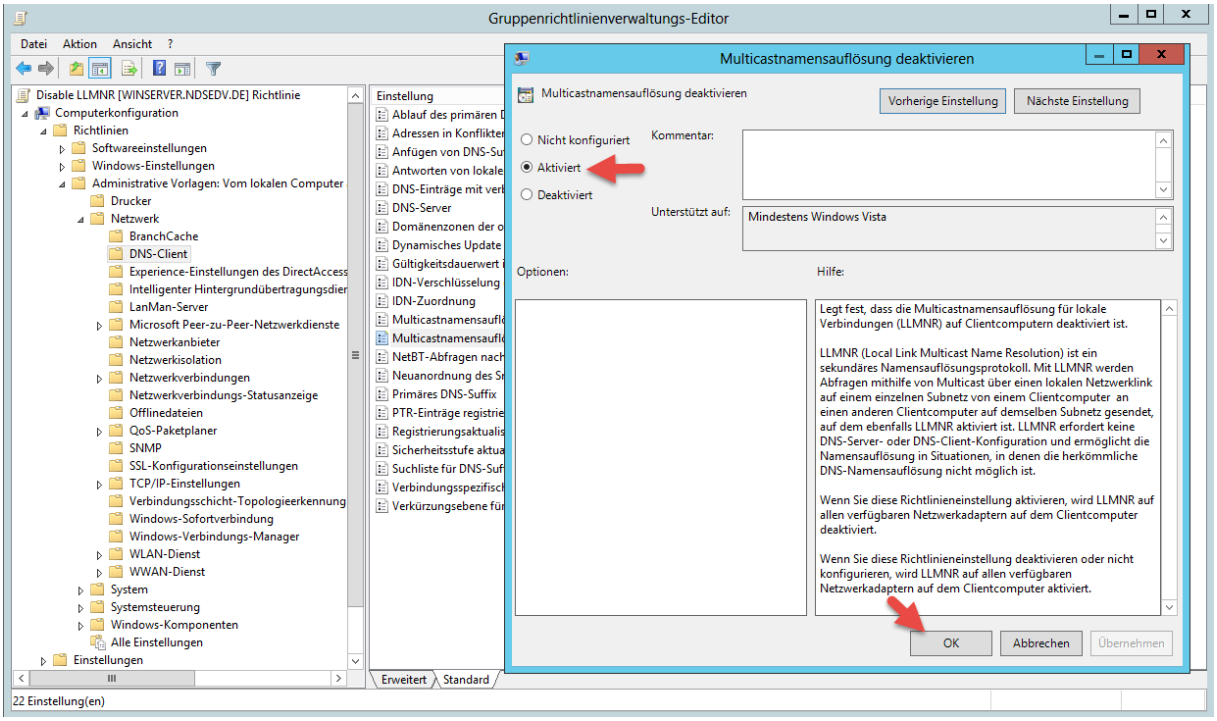
Zum Abschalten von LLMNR gehen wir wie folgt vor:

Anlegen eine neuen **GPO** namens **Disable LLMNR**.

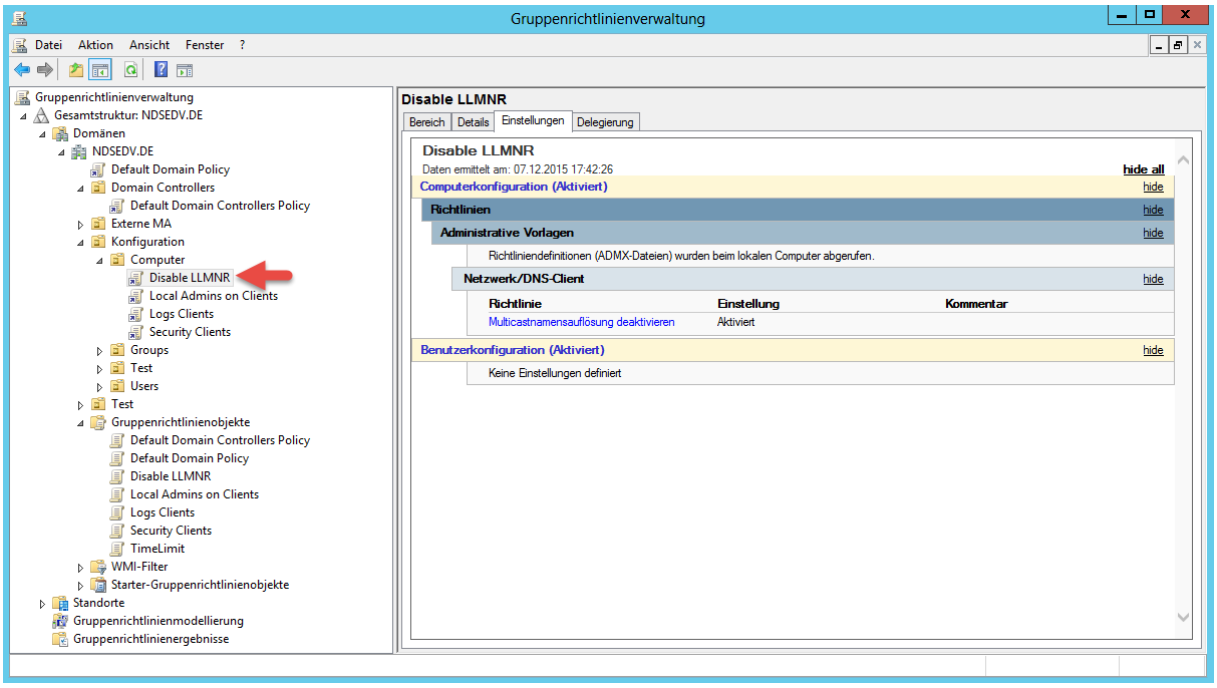
Computerconfiguration > Administrative Templates > Network > DNC Client



Doppelklick und > **auf Enabled** setzen.



Die neue GPO wird auf dann z.B. auf die OU **Computer** verlinkt.



GPO Bericht:

Disable LLMNR

Daten ermittelt am: 07.12.2015 17:42:26 — hide all

Allgemein — hide

Details — hide

Domäne	NDSEDV.DE
Besitzer	NDSEDV\Domänen-Admins
Erstellt	07.12.2015 17:36:50
Geändert	07.12.2015 17:41:14
Benutzerrevisionen	0 (AD), 0 (SYSVOL)
Computerrevisionen	1 (AD), 1 (SYSVOL)
Eindeutige ID	{55C63924-CB65-42B5-8D73-81AA6898C238}
GPO-Status	Aktiviert

Verknüpfungen — hide

Standort	Erzwungen	Verknüpfungsstatus	Pfad
Computer	Nein	Aktiviert	NDSEDV.DE/Konfiguration/Computer

Die Liste enthält Verknüpfungen zur Domäne des Gruppenrichtlinienobjekts.

Sicherheitsfilterung — hide

Die Einstellungen dieses Gruppenrichtlinienobjekts können nur auf folgenden Gruppen, Benutzer und Computer angewendet werden:

Name
NT-AUTORITÄT\Authentifizierte Benutzer

Delegierung — hide

Folgende Gruppen und Benutzer haben die angegebene Berechtigung für das Gruppenrichtlinienobjekt

Name	Zulässige Berechtigungen	Geerbt
NDSEDV\Domänen-Admins	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NDSEDV\Organisations-Admins	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NT-AUTORITÄT\Authentifizierte Benutzer	Lesen (durch Sicherheitsfilterung)	Nein
NT-AUTORITÄT\DOMÄNENCONTROLLER DER ORGANISATION	Lesen	Nein
NT-AUTORITÄT\SYSTEM	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein

Computerkonfiguration (Aktiviert) — hide

Richtlinien — hide

Administrative Vorlagen — hide

Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Computer abgerufen.

Netzwerk/DNS-Client — hide

Richtlinie	Einstellung	Kommentar
Multicastnamensauflösung deaktivieren	Aktiviert	

Benutzerkonfiguration (Aktiviert) — hide

Keine Einstellungen definiert