Schatten DNS - Konfigurationshilfe Windows

06.07.2025 10:54:30

FAQ-Artikel-Ausdruck

Kategorie:	Datennetz::DNS	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	11:34:15 - 01.07.2025

Schlüsselwörter

DNS DNS-Resolver DNS-Server Schatten-DNS

Lösung (öffentlich)

Migration der _msdcs DNS-Zone

Standartmäßig wird neben der DNS-Zone für die Windows-Domäne (im Beispiel "meine-domaene.tu-dresden.de") auch eine weitere DNS-Zone für die _msdcs Sub-Domain angelegt, worin sich die DNS-Einträge zur Ermittlung der zuständigen DCs für die Windows-Domäne befinden. Diese separate DNS-Zone ermöglicht es diese DC-Zuständigkeiten zu replizieren, und das unabhängig von der eigentlichen DNS-Zone der Windows-Domäne mitsamt allen ihrer DNS-Einträge. Es gibt aber keine (technische) Notwendigkeit dass diese _msdcs Sub-Domain eine separate DNS-Zone sein muss, aber leider hält sich auch hier hartnäckig die weitverbreitete Fehlannahme dass das zwangsläufig so sein muss. An den DNS-Einträgen (überwiegend SRV) ist auch nichts speziell oder besonders, sie werden wie alle anderen DNS-Einträge ganz normal über DNS-Anfragen abgefragt.

Der Vorteil von unabhängiger Replikation ist für das hier verfolgte Ziel nicht relevant, da sowieso die gesamte DNS-Zone der Windows-Domäne transferiert werden soll. Im Gegenteil ist es sogar ein Nachteil, weil dadurch zwei Zonen transferiert werden müssen.

Falls es eine separate _msdcs DNS-Zone gibt, muss diese deshalb in die Haupt-Zone migriert werden. Leider bietet Microsoft für diesen Vorgang keine einfache und komfortable Lösung. Als Hilfsmittel stellen wir [1]als GitLab-Snippet ein PowerShell-Skript zur Verfügung, welches auf einem der DCs ausgeführt werden muss. Das Skript kann problemlos während dem laufenden Betrieb ausgeführt werden, es sind keine Neustarts von Diensten oder Hosts notwendig. Am Ende sollte die _msdcs DNS-Zone nicht mehr existieren, und deren DNS-Einträge liegen in der DNS-Zone der Windows-Domäne.

Mit folgendem Befehl lässt sich überprüfen, ob die Windows-Domäne bzw. seine DCs (noch) über DNS ermittelt werden können. Damit dies funktioniert, muss der ausführende Host die entsprechenden _msdcs DNS-Einträge auf den DCs auflösen können; sei es direkt weil er die DCs als DNS-Server verwendet, oder indirekt über den konfigurierten rekursiven DNS-Server.

nltest /dsgetdc:meine-domaene.tu-dresden.de /force

Zonen-Transfer

Standardmäßig tragen sich die DCs immer wieder selbst als autoritative DNS-Server ein. Selbst wenn man diese manuell löscht, fügen sie sich nach einiger Zeit wieder von selbst hinzu. Dies muss man deaktivieren indem man den folgenden Befehl auf allen DCs ausführt:

dnscmd localhost /config /DisableNSRecordsAutoCreation 1

Hinweis: Dadurch wird nicht nur die Wieder-Neuanlage unterbunden, sondern auch der existierende NS-Eintrag aktiv entfernt. Dadurch werden auch manuell angelegte NS-Einträge für die DCs immer wieder entfernt.

Über den DNS-Manager kann man nun die Zone wie gewünscht konfigurieren. Die Einstellungen für eine Zone findet man über Rechtsklick - Eigenschaften.

Im Reiter "Zonenübertragung" muss der Haken bei "Zonenübertragung zulassen" gesetzt sein, und der Modus "Nur an folgende Server" ausgewählt sein. In der Server-Liste ist unser DNS-Einliefer-Server (pdns1.zih.tu-dresden.de bzw. 141.76.10.196) eingetragen. Das rote Kreuz beim Anlegen ist leider normal, und kann ignoriert werden.

Über den Button "Benachrichtigungen" wird ein neues Fenster geöffnet. Dort muss der Haken bei "Automatisch benachrichtigen" gesetzt sein, und der Modus "Folgende Server" ausgewählt sein. In der Server-Liste ist unser DNS-Einliefer-Server (pdns1.zih.tu-dresden.de bzw. 141.76.10.196) eingetragen. Auch hier kann das rote Kreuz ignoriert werden.

Im Reiter "Autoritätsursprung (SOA)" muss unter "Primärer Server" einer der Domänencontroller eingetragen sein, sowie unter "Verantwortliche Person" und den vier Zeitangaben die angegeben Werte.

Im Reiter "Namenserver" müssen in der Server-Liste je nach Zonen-Typ die vier öffentlichen bzw. zwei internen DNS-Server eingetragen sein.

Rekursion abschalten

Um die Beantwortung rekursiver DNS-Anfragen zu deaktiveren, muss man im DNS-Manager die Einstellungen des DNS-Servers über Rechtsklick - Eigenschaften öffnen.

Im Reiter "Erweitert" kann dann die Serveroption "Rekursionsvorgang (und Weiterleitungen) deaktivieren" aktiviert werden.

Wichtig: Es müssen vorher alle Clients (inkl. Gruppenlaufwerke, DHCP-Server, VPNs, auch die DCs selbst!) umkonfiguriert werden, sodass diese als DNS-Server nicht mehr die DCs sondern andere DNS-Resolver (normalerweise die des ZIH) verwenden. Außerdem muss der Zonen-Transfer bereits vollständig eingerichtet sein (auch auf ZIH Seite!) und funktionieren.

[1] https://gitlab.hrz.tu-chemnitz.de/-/snippets/237