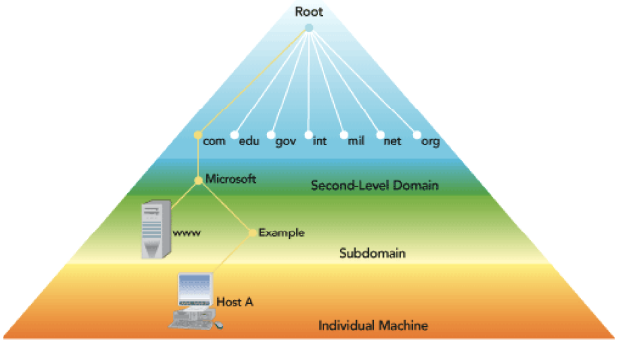
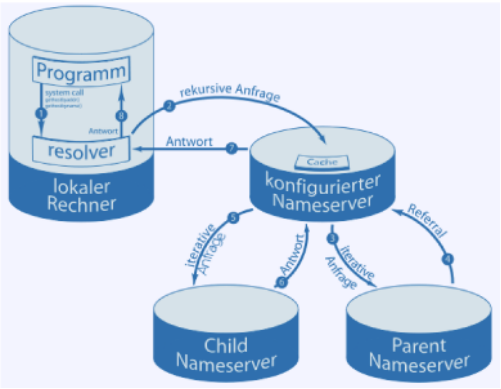
-DNS (Domain Name System)



Das DNS ist ein weltweit auf tausende von Servern verteilter hierarchischer Verzeichnisdienst, der den Namensraum des Internets verwaltet. Dieser Namensraum ist in so genannte Zonen unterteilt, für die jeweils unabhängige Administratoren zuständig sind. Für lokale Anforderungen – etwa innerhalb eines Firmennetzes – ist es auch möglich, ein vom Internet unabhängiges DNS zu betreiben.Hauptsächlich wird das DNS zur Umsetzung von Domainnamen in IP-Adressen (*„forward lookup“*) benutzt. Dies ist vergleichbar mit einem Telefonbuch, das die Namen der Teilnehmer in ihre Telefonnummer auflöst. Das DNS bietet somit eine Vereinfachung, weil Menschen sich Namen weitaus besser merken können als Zahlenkolonnen.

-Resolver



Resolver sind einfach aufgebaute Software-Module, die auf dem Rechner eines DNS-Teilnehmers installiert sind und die Informationen von Nameservern abrufen können. Sie bilden die Schnittstelle zwischen Anwendung und Nameserver. Der Resolver übernimmt die Anfrage einer Anwendung, ergänzt sie, falls notwendig, zu einem FQDN und übermittelt sie an einen normalerweise fest zugeordneten Nameserver. Ein Resolver arbeitet entweder rekursiv oder iterativ.

-rekursive Abfrage

Im rekursiven Modus schickt der Resolver eine **rekursive Anfrage** an den ihm zugeordneten Nameserver. Hat dieser die gewünschte Information nicht im eigenen Datenbestand, so kontaktiert der Nameserver weitere Server, und zwar solange bis er entweder eine positive Antwort oder bis er von einem autoritativen Server eine negative Antwort erhält. Rekursiv arbeitende Resolver überlassen also die Arbeit zur vollständigen Auflösung ihrem Nameserver.

C:\Windows\System32\DNS\Cache.DNS - Alle Stammserver „Stammhinweise“ aufgelistet

-iterative Abfragen

-Bei einer **iterativen Anfrage** bekommt der Resolver entweder den gewünschten Resource Record oder einen Verweis auf weitere Nameserver, die er als nächstes fragt. Der Resolver hangelt sich so von Nameserver zu Nameserver, bis er von einem eine verbindliche Antwort erhält.

Die so gewonnene Antwort übergibt der Resolver an das Programm, das die Daten angefordert hat, beispielsweise an den Webserver. Übliche Resolver von Clients arbeiten ausschließlich rekursiv, sie werden dann auch als Stub-Resolver bezeichnet. Nameserver besitzen in der Regel eigene Resolver. Diese arbeiten gewöhnlich iterativ

-Weiterleitungsserver

-Ein Weiterleitungsserver ist ein von anderen internen DNS Servern bestimmter DNS Server für die Weiterleitung von Abfragen zur Auflösung von externen und Offsite-DNS-Domänennamen (steht z.B in DMZ)

-Zwischenspeicherung auf dem DNS-Server

-Zwischenspeichern ist die termporäre Speicherung von kürzlich angeforderten Informationen in einem speziellen Arbeitsspeichersubsystem für schnelleren Zugriff

-Speicherung und Verwaltung von DNS-Daten

-Ressourceneinträge und Eintragstypen

-A: Löst einen Hostnamen in eine IP-Adresse auf
-PTR: Löst eine IP-Adresse in einen Hostnamen auf
-SOA: Der erste Eintrag in jeder Zonendatei
-SRV: Löst Namen von servern auf, die Dienste anbieten
-NS: Identifiziert den DNS-Server für jede Zone
-MX: Der Mailserver
-CNAME: Löst einen Hostnamen in einen Hostnamen auf

(-AAAA: IPv6 löst Hostnamen in IP-Adressen auf)

-Was ist eine DNS-Zone

-Im DNS des Internets bezeichnet **Zone** den Teil des Domänenbaums, für die ein Nameserver zuständig ist und deshalb die offiziellen Daten kennt. Eine Zone wird durch einen Primary Nameserver verwaltet.

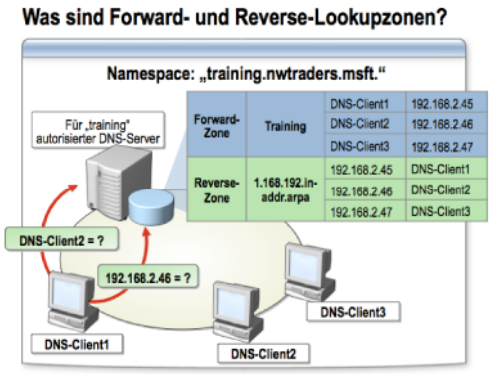
-DNS-Zonentypen

-Primäre „Lesen/Schreiben“: Lese/Schreibkopie einer DNS-Datenbank
-Sekundäre „Schreibgeschützt“: Schreibgeschützte Kopie einer DNS-Datenbank
-Stub „Kopie begrenzter Einträge“: Kopie einer Zone mit begrenzten Einträgen

-Forward und Reverse-Lookupzoenen

- Forward-Zonen sind das, was du als DNS kennst, nämlich Name -> IP-Adresse.

-Reverse-Zonen machen genau das Gegenteil. Das löst IP-Adressen zu Namen auf (und wird meistens vergessen).



-DNS Zonenübertragung

-Eine DNS.Zonenübertragung bezeichnet das Synchronisieren autorisierender DNS-Zonendaten zwischen DNS-Server
-IXFR = Inkrementeller Zonentransfer
-AXFR = Vollständiger Zonentransfer

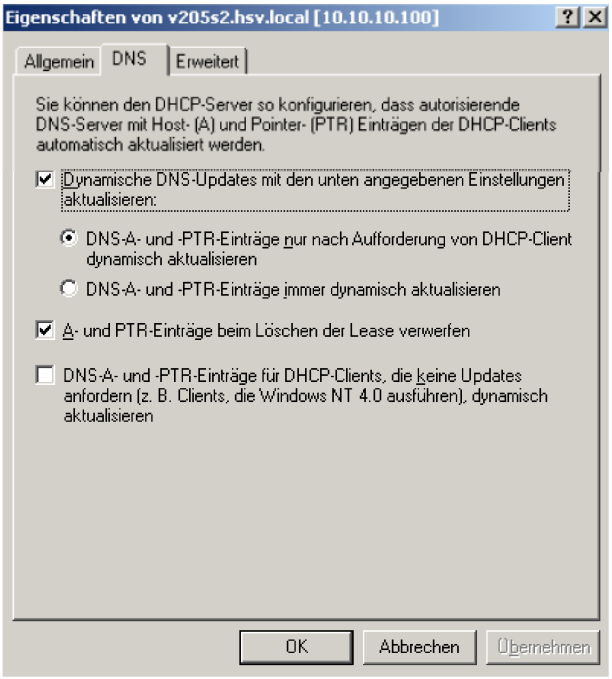
-DNS-Benachrichtigungen

-Die DNS-Benachrichtigungen ist eine Aktualisieren der ursprünglichen DNS. Protokollspezifikation, die eine Benachrichtigung der sekundären Server bei Zonenänderungen ermöglicht

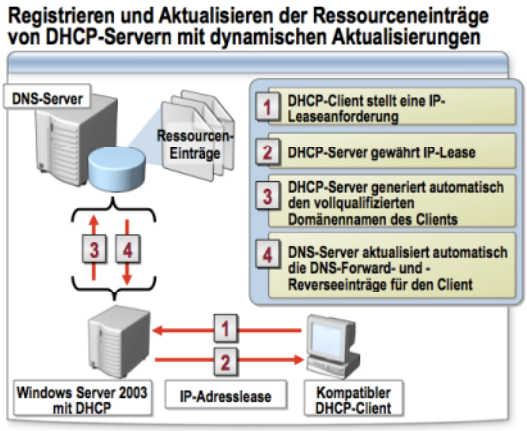
-dynamische Aktualisierungen

-Eine dynamische Aktualisierung ist das dynamische Erstellen, Registrieren oder Aktualisieren der Einträge eines DNS.Clients in Zonen, die von DNS-Server verwaltet werden, die Nachrichten für dynamische Aktualisierungen annehmen und verarbeiten können.
-Eine manuelle Aktualisierung ist das manuelle Erstellen, Registrieren oder Aktualiesieren der Ressourceneinträge durch den Administrator

DHCP-Server kann automatisch Aktualisierungen am DNS Server vornehmen

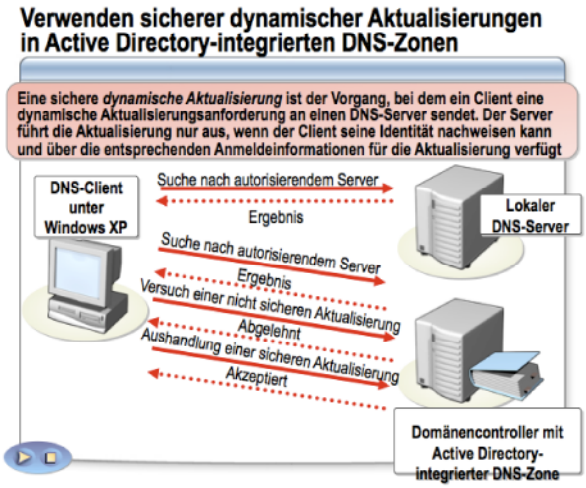


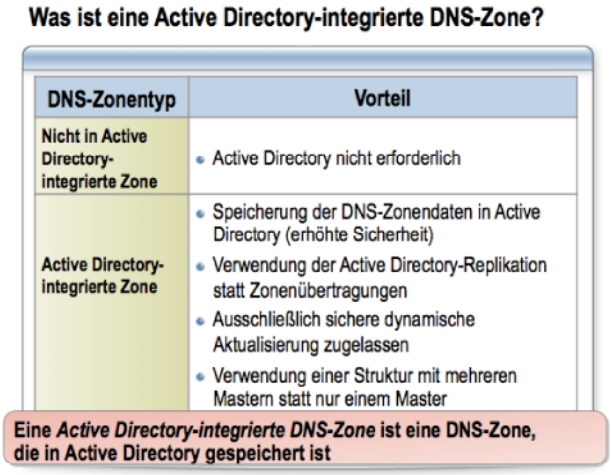
(Eigenschaften von DHCP-Server)



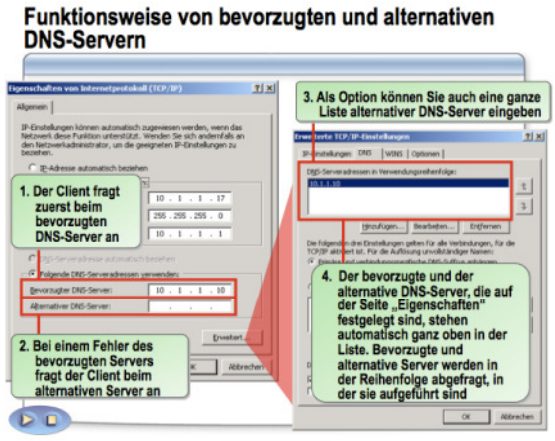
-Active Directory-integrierte DNS-Zone

-Eine Active Directory-integrierte DNS-Zone ist eine DNS-Zone, die in Active Directory gespeichert ist

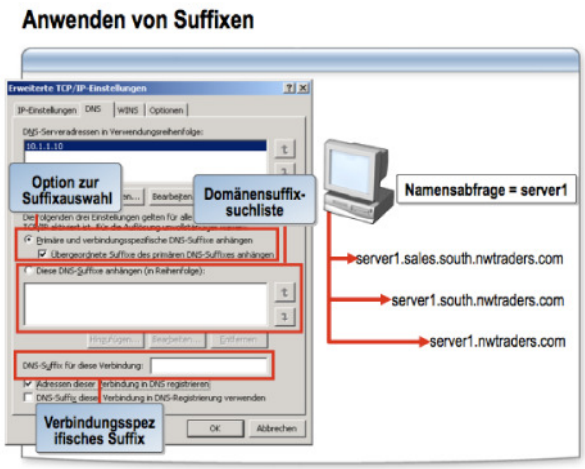




-Konfigurieren DNS-Clients

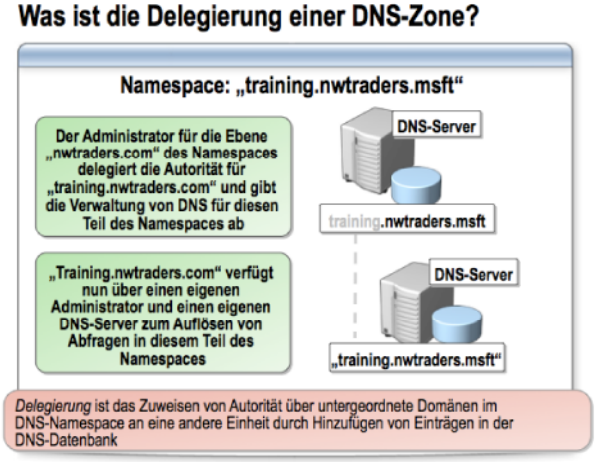


-Anwenden von Suffixen



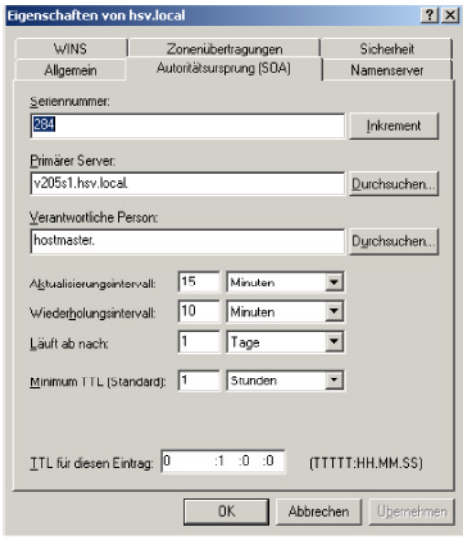
-Delegieren der Autorität einer DNS-Zone

-Untergeordnete Domänenzonen können an andere Server delegiert werden

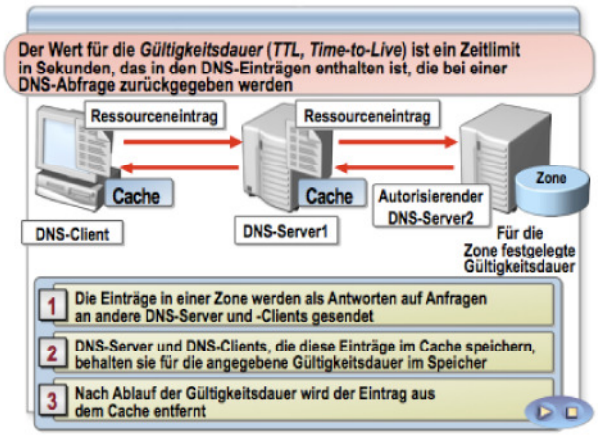


-Gültigkeitsdauer

-Der Wert die Gültigkeitsdauer (TTL, Time to Live) ist ein Zeitlimit in Sec. Das in den DNS-Einträgen enthalten ist, die bei einer DNS-Abfrage zurückgegeben werden.



Funktion der Gültigkeitsdauer

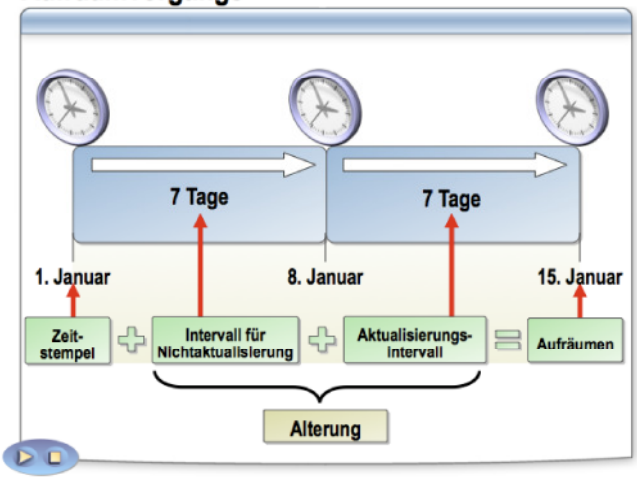


-Parameter für Alterung und Aufräumvorgang

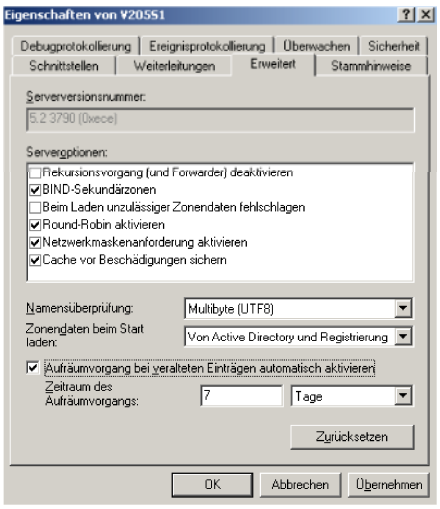
-Anhand der Alterung wird bestimmt, ob ein veralteter DNS-Resourceneintrag aus der DNS-Datenbank entfernt werden soll
-Beim Aufräumvorgang werden die abgelaufenen oder veralteten Namensdaten in der WINS-Datenbank bereinigt oder entfernt
-Bei einem Aktualisierungsversuch fordert ein Computer eine Aktualisierung seines DNS-Eintrags an

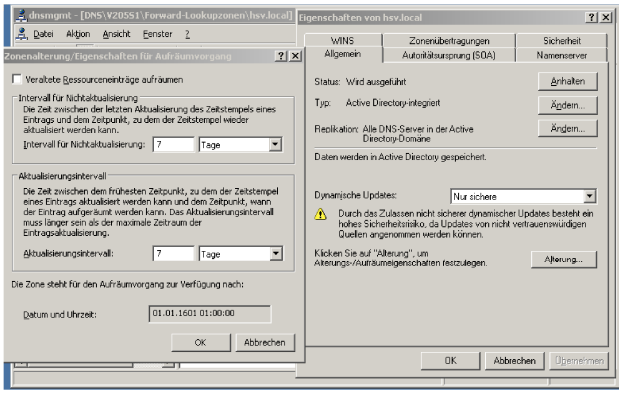
-Parameter:
-Intervall für Nichtaktualisierung: Die Zeitspanne, vor deren Ablauf der DNS-Server keine Aktualisierungsversuche aktualisiert (7 Tage Stand.)
-Aktualisierungsintervall: Die Zeitspanne, bis zu deren Ablauf der DNS-Server Aktualisierungsversuche akzeptiert (7 Tage Stand.)

Funktionsweise der Alterung und des Aufräumvorgangs



-Alterung kann für den gesamten DNS-Server oder für einzelne Zonen eingestellt werden

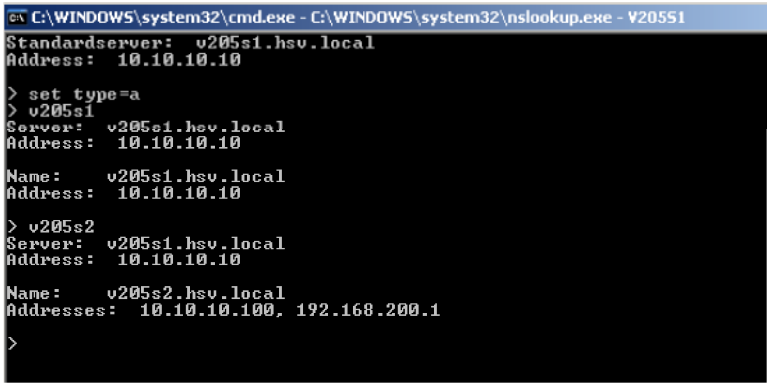




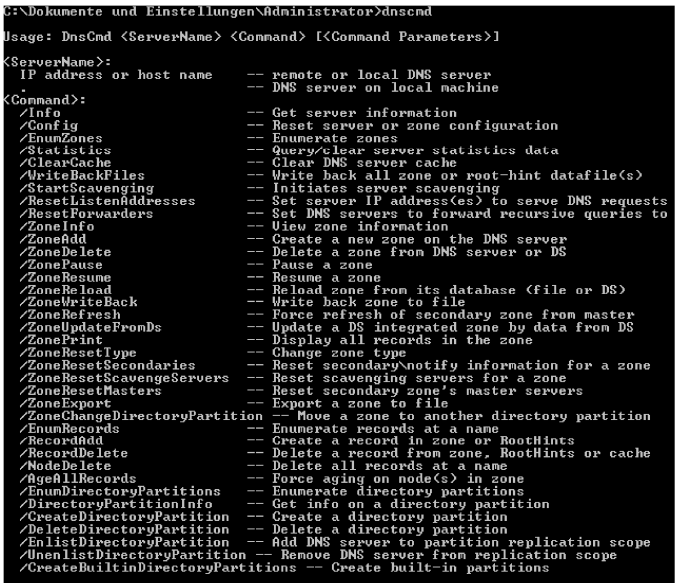
-Alterung muss im DNS-Server unter Eigenschaften -> erweitert

-DNS Diagnose

-CMD: nslookup



-CMD: dnscmd



-Überwachen der DNS-Serverleitung

Richtlinien für die Überwachung der DNS-Serverleistung mithilfe der Leistungskonsole

Leistungsindikator	Zu berücksichtigende Aspekte nach Einrichten einer Baseline
Verweigerte dynamische Aktualisierungen	Jegliches Ansteigen über die Baseline gibt Anlass für weitere Untersuchungen
Rekursive Abfragen/Sek.	Ein beträchtliches Ansteigen oder Abfallen dieses Indikators gibt Anlass für weitere Untersuchungen
Gesendete AXFR-Anforderungen	Wenn dieser Indikator die Baseline beträchtlich übersteigt, kann dies Anlass für eine Überprüfung der Anzahl der Änderungen in der Zone und der Konfiguration der Zonenübertragungen sein

-DNS-Debugprotokollierung

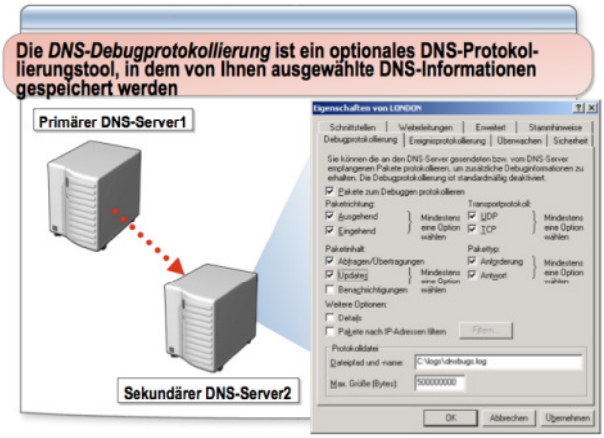
-Die DNS-Debugprotokollierung ist ein optionales DNS-protokollierungstool, in dem von Ihnen ausgewählte DNS-Informationen gespeichert werden.
(Eigenschaften von DNS-Server)

ACHTUNG: Protokollierung erhöht immer die Last auf dem Server.

Logdatei in:

c:\windows\system32\dns\dns.log

Was ist DNS-Debugprotokollierung?



-DNS Ereignisprotokoll

Was ist ein DNS-Ereignisprotokoll?

