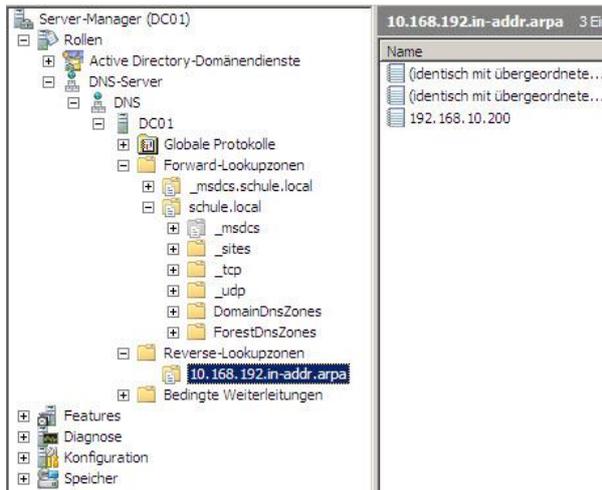


3. Netzwerkdienste im AD-Umfeld: DNS

3.1. DNS

Bei der Installation des Active Directory wurde der DNS mit eingerichtet. Auch auf dem zusätzlichen Domänencontroller wurde der DNS installiert. Nun müssen noch ein paar Einstellungen gemacht werden und die korrekte Funktion überprüft werden.

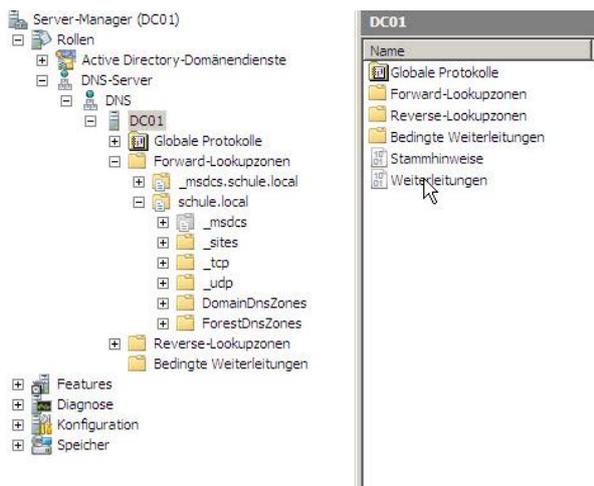
Rufen sie über den Server Manager den DNS Server auf und erweitern sie die Ansicht:



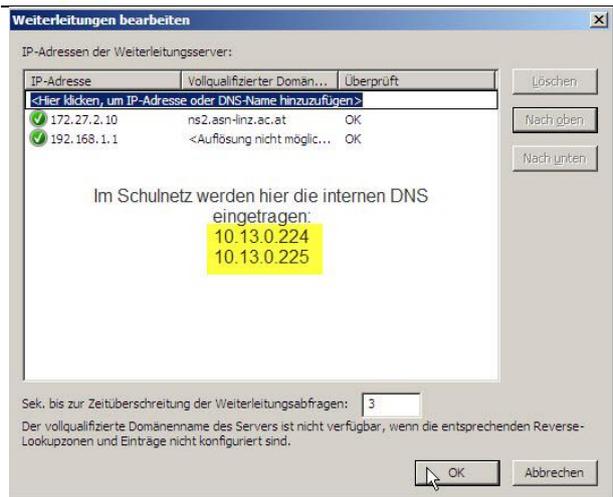
3.1.1. Weiterleitung

Als erstes konfigurieren wir die DNS Weiterleitung. Achtung bei Windows Server 2008 gibt es auch eine bedingte Weiterleitung, die wir aber vorerst nicht verwenden.

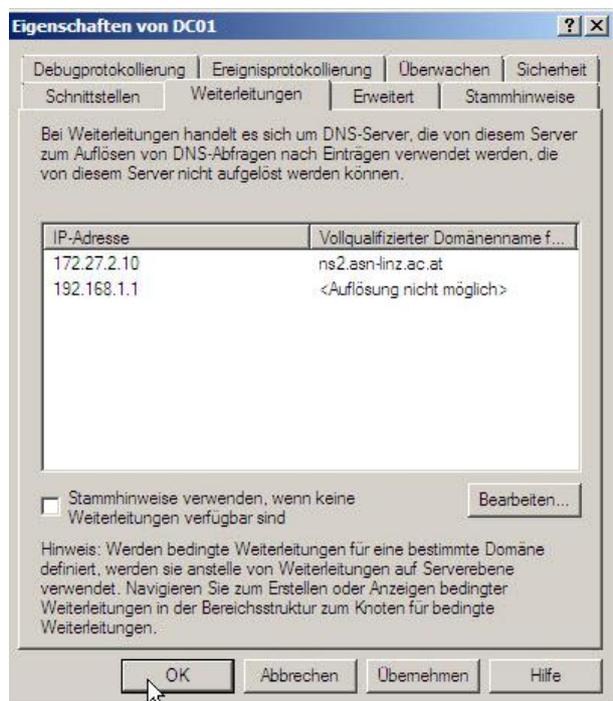
Klicken sie auf den DNS Server (DC01) und im rechten Fenster auf Weiterleitungen



Nun werden die DNS Server, an die die Weiterleitung gerichtet ist eingetragen



OK



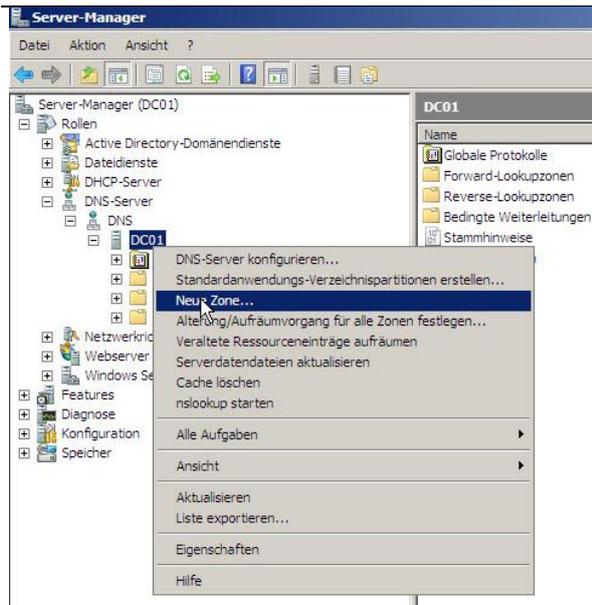
OK

3.1.2. Reverse-Lookupzone einrichten

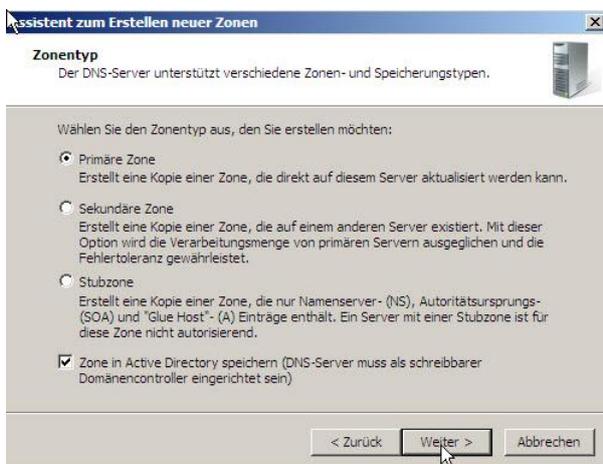
Eine Reverse-Lookupzone dient zum Auflösen von IP-Adressen in Hostnamen. Diese Funktionalität ist zwar nicht unbedingt notwendig, trotzdem macht es Sinn, zumal sie mit wenigen Handgriffen eingerichtet ist.

Im DNS-Manager können Sie über den Menüpunkt Neue Zone einen Assistenten aufrufen, der das Anlegen einer Reverse-Lookupzone maximal einfach macht.

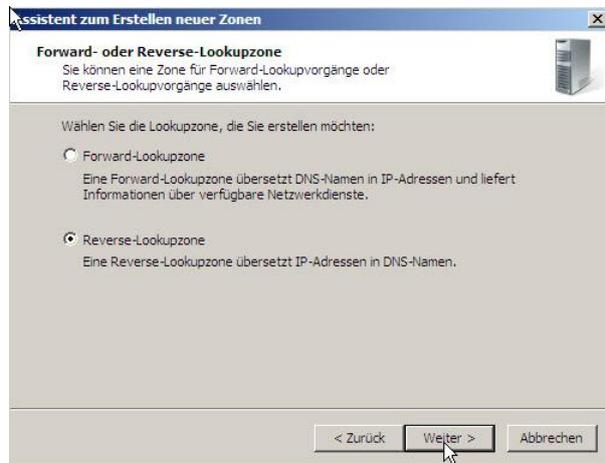
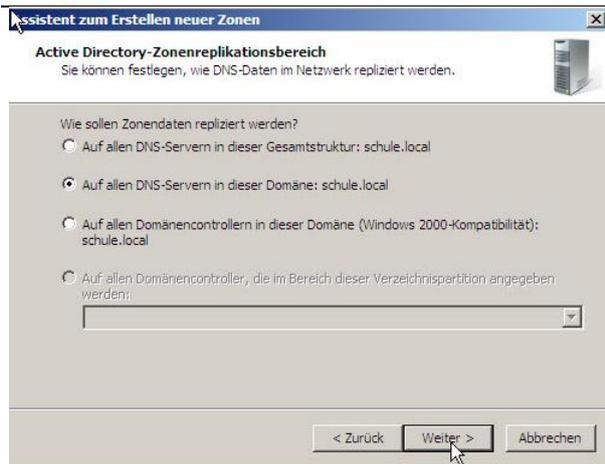
Die wesentlichen Schritte des Assistenten sind folgende:



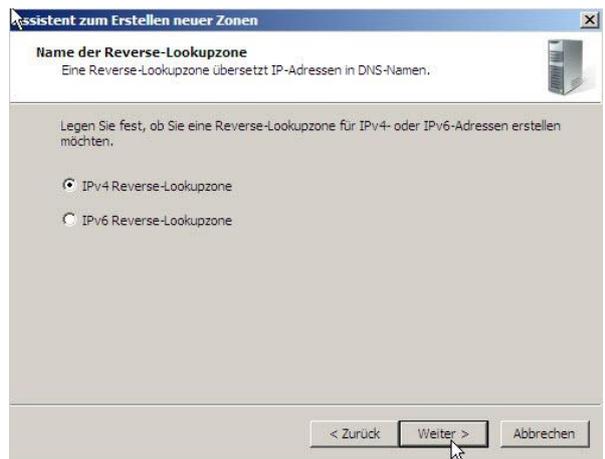
Zunächst müssen Sie den Zonentyp auswählen. Im Normalfall wird eine Active Directory-integrierte Zone ausgewählt, diese muss notwendigerweise eine Primäre Zone sein



Auf der nächsten Dialogseite konfigurieren Sie, in welchem Replikationsbereich die Zone verteilt werden soll: Gesamtstruktur oder Domäne. Falls Sie Windows 2000-Domänencontroller einsetzen, müssen Sie die dritte Option auswählen



Die folgende Dialogseite dient zur Auswahl, ob Sie eine IPv4- oder eine IPv6-Reverse-Lookupzone erstellen möchten. Wenn Sie sowohl IPv4 als auch IPv6 einsetzen, benötigen Sie zwei Reverse-Lookupzonen. (Führen Sie einfach den Assistenten zweimal aus)



Sie müssen lediglich die Netzwerk-ID, also die IP-Adresse des Netzes, eingeben.

Assistent zum Erstellen neuer Zonen

Name der Reverse-Lookupzone

Eine Reverse-Lookupzone übersetzt IP-Adressen in DNS-Namen.

Geben Sie die Netzwerk-ID oder den Namen der Reverse-Lookupzone an.

Netzwerk-ID:
[192 .168 .10] .

Die Netzwerk-ID ist der Teil der IP-Adresse, der dieser Zone angehört. Geben Sie die Netzwerk-ID in ihrer normalen Reihenfolge (nicht umgekehrt) ein.

Wenn Sie eine Null in der Netzwerk-ID verwenden, wird diese im Zonennamen angezeigt. Beispiel: Netzwerk-ID 10 erstellt Zone 10.in-addr.arpa und Netzwerk-ID 10.0 erstellt Zone 0.10.in-addr.arpa.

Name der Reverse-Lookupzone:
10.168.192.in-addr.arpa

< Zurück Weiter > Abbrechen

Assistent zum Erstellen neuer Zonen

Dynamisches Update

Sie können festlegen, dass diese DNS-Zone sichere, unsichere oder keine dynamische Updates zulässt.

Dynamische Updates ermöglichen DNS-Clientcomputern, sich zu registrieren und die eigenen Ressourceneinträge dynamisch mit einem DNS-Server bei Änderungen zu aktualisieren.

Bestimmen Sie den Typ des dynamischen Updates, der verwendet werden soll.

Nur sichere dynamische Updates zulassen (für Active Directory empfohlen)
Diese Option ist nur für Active Directory-integrierte Zonen verfügbar.

Nicht sichere und sichere dynamische Updates zulassen
Dynamische Updates von Ressourceneinträgen werden von allen Clients zugelassen.
 Durch diese Option besteht ein hohes Sicherheitsrisiko, da Updates von nicht vertrauenswürdigen Quellen angenommen werden können.

Dynamische Updates nicht zulassen
Dynamische Updates von Ressourceneinträgen werden von dieser Zone nicht zugelassen. Diese Einträge müssen manuell aktualisiert werden.

< Zurück Weiter > Abbrechen

Assistent zum Erstellen neuer Zonen

Fertigstellen des Assistenten

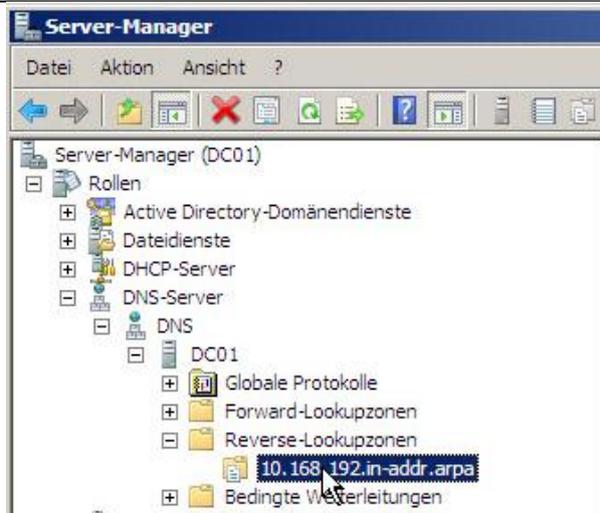
Der Assistent zum Erstellen neuer Zonen wurde erfolgreich abgeschlossen. Folgende Einstellungen wurden festgelegt:

Name: "10.168.192.in-addr.arpa"
Typ: "Active Directory-integriert, primär"
Lookuptyp: "Umkehren"

Hinweis: Sie sollten jetzt der Zone Einträge hinzufügen oder sich vergewissern, dass die Einträge dynamisch aktualisiert werden. Danach können Sie die Namensauflösung mit nslookup verifizieren.

Klicken Sie auf "Fertig stellen", um die neue Zone zu erstellen und den Vorgang abzuschließen.

< Zurück Fertig stellen Abbrechen



Ob das Reverse-Lookup funktioniert, können Sie recht einfach mittels Ping prüfen. Der Aufruf muss ping -a [adresse] lauten.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. Alle Rechte vorbehalten.
C:\Users\Administrator>ping -a 192.168.10.200

Ping wird ausgeführt für DC01.schule.local [192.168.10.200] mit 32 Bytes Daten:
Antwort von 192.168.10.200: Bytes=32 Zeit<1ms TTL=128

Ping-Statistik für 192.168.10.200:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
```