1 Die Namensauflösung mit DNS

Prüfungsanforderungen von Microsoft:

- Implement DNS
    - Install and Configure DNS-Servers
    - Create and Configure DNS Zones and Records

Quelle: Microsoft

Lernziele:

- DNS Zonen
- Überprüfen der DNS Konfiguration
- Weitere Konfiguration des Servers
- Delegieren von Zonen und Erstellen einer Stubzone
- Sicherheit für DNS
- DNS und WINS: GlobalNamesZone
- DNS Richtlinien
- Die Namensauflösung aus der Sicht der Clients

1.1 Einführung

Im DNS-Server ist die Zuordnung von Namen zu IP-Adressen gespeichert.

Ein DNS-Server ist unterteilt in eine Forward-Lookupzone und in eine Reverse-Lookupzone. Außerdem ist die Ereignisanzeige für die DNS-Ereignisse hier noch einmal eingegliedert.

Die Namensauflösung ist die Zuordnung von benutzerfreundlichen Computernamen zu deren IP-Adressen, mit denen das Protokoll IP arbeitet.

Es gibt statische und dynamische Namensauflösung.

Die Reihenfolge der Namensauflösung ist bei modernen Windows-Rechnern folgendermaßen:

1. Local Host Name

2. Datei „Hosts“

3. DNS-Server

4. NetBios Namenscache

5. WINS

6. Broadcast

7. Datei „LMHosts“

Abbildung 1.1: Die Reihenfolge der Namensauflösung

ACHTUNG!
Vor Windows 2000 gab es eine andere Reihenfolge der Namensauflösung, diese spielt aber mittlerweile keine Rolle mehr, da es kaum noch ältere Clients gibt.

1.2 Forward-Lookupzone

Die Forward-Lookupzone löst die Namen zu IP-Adressen auf. Ähnlich wie in einer Telefonbuchliste ist jedem Namen eine Nummer zugeordnet.

Dies ist der Normalfall. Wenn mit dem Computer im Netzwerk gearbeitet wird, sprechen wir die Computer, die wir erreichen möchten, immer mit dem Namen an.

Das Protokoll IP benötigt aber zum Routen die IP-Adresse. Also wird in der Namensauflösung der Name zu einer IP-Adresse aufgelöst.

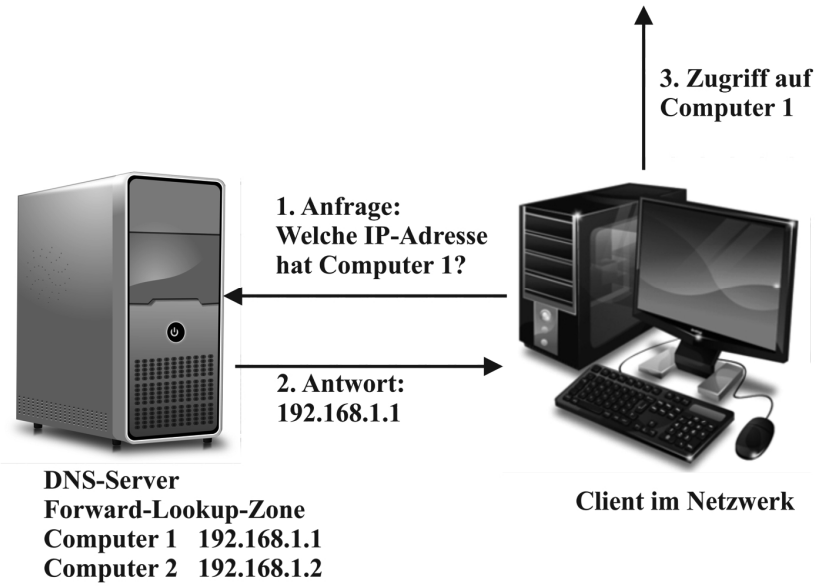

Abbildung 1.2: Namensauflösung mit DNS

1.3 Reverse-Lookupzone

Die Reverse-Lookupzone ist genau das Gegenteil: Sie löst IP-Adressen zu Namen auf.

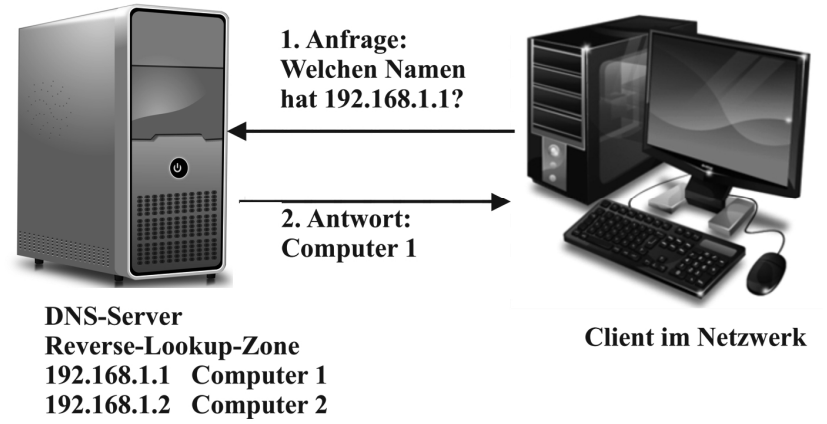

Abbildung 1.3: Reverse-Lookupzone

Die Reverse-Lookupzone wird für den normalen Arbeitsalltag nicht benötigt. Sie wird nur zur Kontrolle und zum Testen benötigt, da

normalerweise nicht nach Namen gefragt wird.

Auch einige Anwendungen benötigen eine Reverse-Lookupzone, falls sie Clients mit Namen analysieren müssen.

Falls Sie eine Serveranwendung installieren, und danach eine Fehlermeldung bekommen, dass die Anwendung Clients nicht mit Namen analysieren kann, ist in den meisten Fällen das Einrichten einer Reverse-Lookupzone nötig!

1.3.1 Der DNS Namensraum

Der DNS Namensraum ist im ganzen Internet gleich. Die Namen werden von hinten nach vorne ergänzt.

In der Domäne Meistertrainer.info, die ja unser Schulungsbeispiel ist, kann der Namensraum folgendermaßen dargestellt werden:

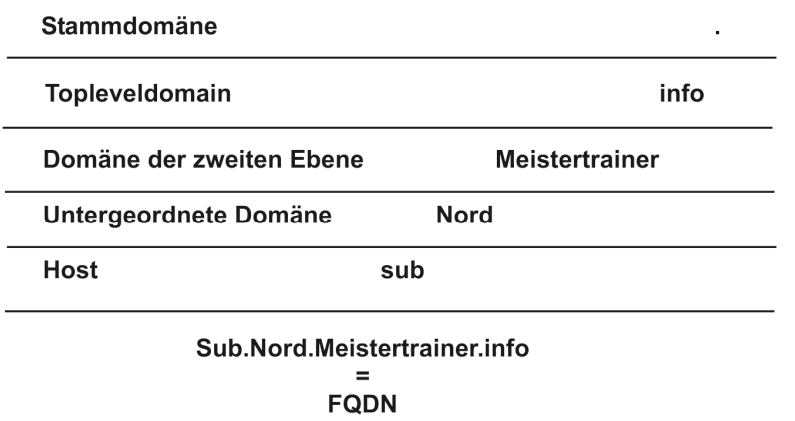

Abbildung 1.4: Der DNS Namensraum

Was im Kleinen funktioniert, ist im Großen das gleiche Prinzip. Auch im Internet wird mit dieser Abstufung der Namen gearbeitet.

Es ist verständlich, dass nicht ein einzelner DNS-Server in der Lage ist, alle diese Namen aufzulösen.

Meistens sind viele DNS-Server an der Auflösung der Namen beteiligt. Wenn ein Server die Antwort nicht kennt, leitet er die Abfrage an einen anderen DNS-Server weiter.

Für die Art und Weise der Antwort gibt es zwei verschiedene Möglichkeiten.

Iterative und rekursive Abfragen

Jeder DNS-Server beherrscht zwei Arten, wie er auf Anfragen der Clients antworten kann.

Iterative Abfrage

Bei der „Iterativen Abfrage“ gibt der DNS-Server die beste Antwort zurück, die er selber geben kann.

Wenn er die gewünschte Information liefern kann, bekommt der Client diese. Wenn der DNS-Server allerdings die Antwort nicht liefern kann, bekommt der Client einen Verweis auf einen weiteren DNS-Server, den er dann kontaktieren kann.

Rekursive Abfrage

Bei einer „Rekursiven Abfrage“ sendet der DNS-Server dem Client die vollständige Antwort auf seine Anfrage.

1.4 Installieren eines DNS-Servers und Erstellen von Zone

Betrachten wir nun, wie ein DNS-Server installiert wird, und wie funktionsfähige Zonen eingerichtet werden.

1.4.1 Installieren des Dienstes

DNS ist ein Netzwerkdienst, und muss dementsprechend installiert werden. Auf Domänencontrollern ist er in den meisten Fällen nach der Installation bereits vorhanden, und eine Forward-Lookupzone ist bereits eingerichtet.

Sollten Sie allerdings den DNS-Dienst auf einem anderen Server installieren wollen, muss er manuell nachinstalliert werden.

DNS ist eine Rolle, die Sie im Servermanager hinzufügen können.

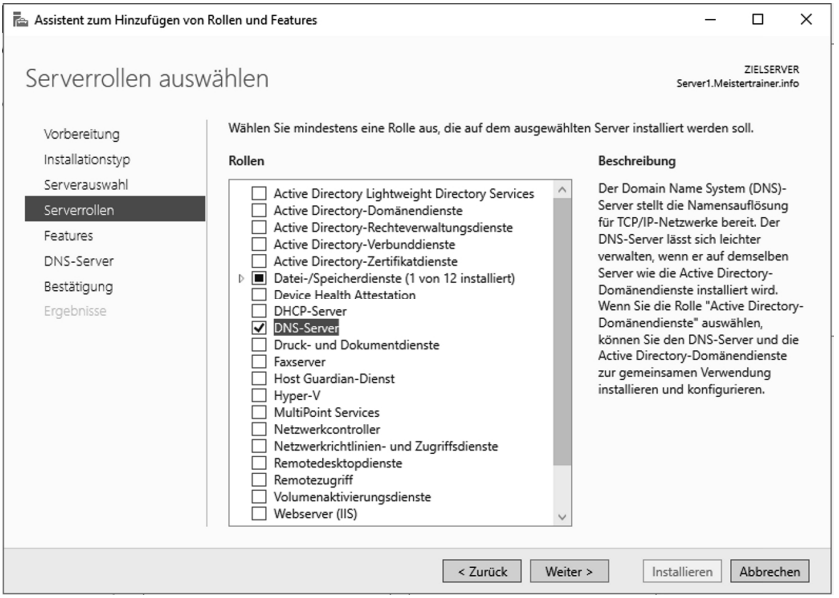

Abbildung 1.5: Installation der DNS-Rolle

Das PowerShell Cmdlet dafür lautet:

Install-WindowsFeature DNS

Nach der erfolgreichen Installation steht Ihnen die DNS-Verwaltungskonsole jetzt in der „Verwaltung“ zur Verfügung.

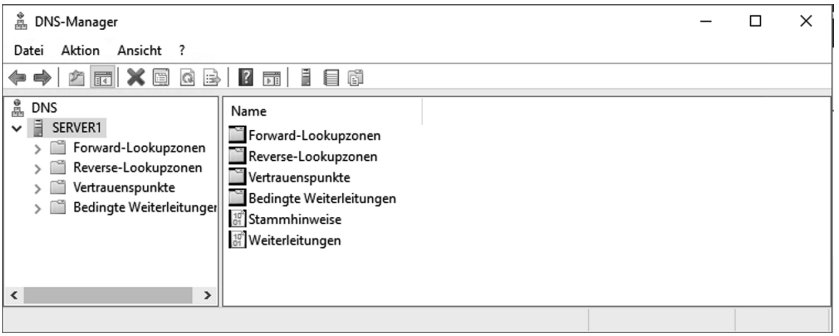

Abbildung 1.6: DNS ist verfügbar

1.4.2 Erstellen von Zonen

Nach der Installation können Sie neue Zonen erstellen. Wir werden dies in unserem Beispiel auf einem Domänencontroller vornehmen, damit Sie den vollen Funktionsumfang sehen können.

Um eine neue Forward-Lookupzone zu erstellen, klicken Sie mit der rechten Maustaste auf „Forward-Lookupzone“ und wählen „Neue Zone“.

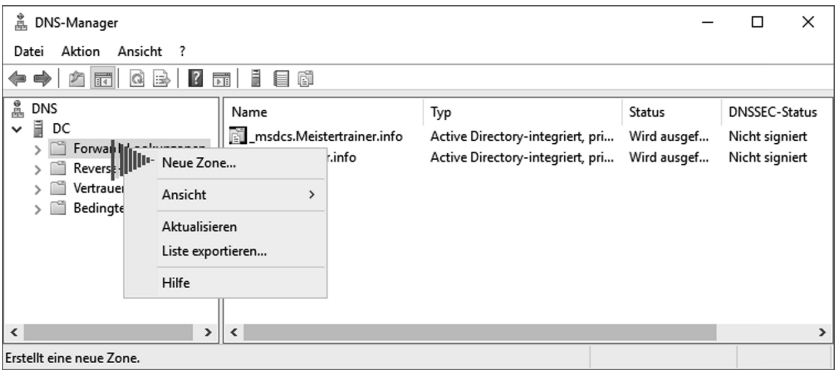

Abbildung 1.7: Neue Zone erstellen

Ein Assistent startet und hilft Ihnen, die Zone einzurichten.

Auf der ersten Seite müssen Sie wählen, welchen Zonentyp Sie für Ihre Forward-Lookupzone benutzen möchten.

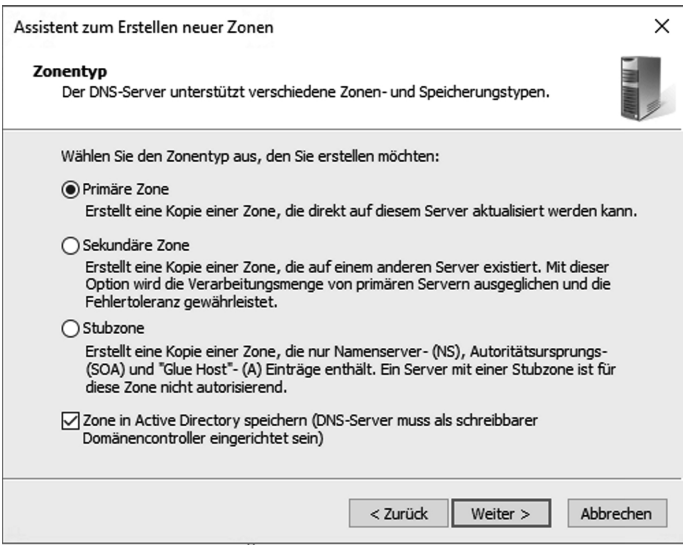

Abbildung 1.8: Auswahl der Zone

Primäre Zone

Eine primäre Zone speichert die Daten in einer Textdatei. Diese Textdatei wird auf dem lokalen Server gespeichert, und ist jederzeit editierbar.

Das PowerShell cmdlet lautet:

Add-DnsServerPrimaryZone

Sekundäre Zone

Eine sekundäre Zone ist eine Textdatei, die von einem DNS-Server mit einer primären Zone kopiert wird, und mit Schreibschutz belegt ist.

Eine sekundäre Zone dient zur Lastenverteilung und zur Fehlertoleranz, sie kann im Fehlerfall der primären Zone alle Anfragen beantworten. Lediglich Änderungen der Daten können an ihr nicht vorgenommen werden, da sie schreibgeschützt ist.

Das PowerShell cmdlet lautet:

Add-DnsServerSecundaryZone

Stubzone

Eine Stubzone enthält Informationen zu delegierten Namenservern.

Das PowerShell cmdlet lautet:

Add-DnsServerStubZone

Zone in Active Directory speichern (DNS-Server muss als schreibbarer Domänencontroller eingerichtet sein)

Dieser Haken kann bei primären Zonen und bei einer Stubzone gesetzt werden. In diesem Fall werden die Informationen nicht in einer Textdatei gespeichert, sondern in die Datenbank Active Directory aufgenommen. Dadurch haben wir einige Vorteile:

- Die Active Directory Replikation kann benutzt werden, die Daten können sehr schnell an andere DNS-Server repliziert werden
- Es muss keine sekundäre Zone zur Fehlertoleranz eingerichtet werden, dadurch entfällt der Single Point of Failure
- Alle DNS-Server, die Active Directory integrierte Zonen haben, haben ein Original der Informationen, und alle Informationen können auf allen DNS-Servern geändert werden

Leider hat diese Auswahl auch einen Nachteil:

- Alle DNS-Server, die Active Directory integriert installiert werden, müssen sich auf einem Domänencontroller befinden, da nur auf einem Domänencontroller das Active Directory vorhanden ist
- Sie können für diese Art der Zone keinen RODC benutzen

Wenn Sie „Active Directory integrierte Zone“ gewählt haben, müssen Sie sich im nächsten Fenster noch für den Replikationsbereich entscheiden.

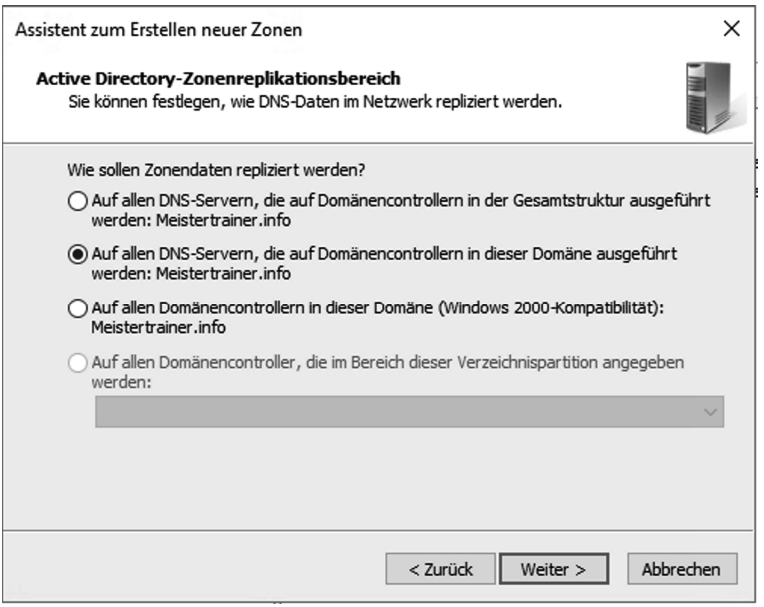

Abbildung 1.9: Replikationsbereich

Durch Festlegen des Replikationsbereichs können Sie steuern, dass nur die DNS-Server der Domäne, der untergeordneten Domäne oder der Gesamtstruktur die Informationen aus DNS erhalten, somit können fremde DNS-Server keine Informationen erhalten.

Auch können Sie an dieser Stelle eine zuvor erstellte eigene Verzeichnispartition wählen. Eine Verzeichnispartition legen Sie auf allen Domänencontrollern an, an die die Informationen repliziert werden sollen.

Der PowerShell Parameter dafür lautet:

-DirectoryPartitionName<String>