PEARSON Education

ADDISON-WESLEY

Frank Castro Lieberwirth

MCSA/MCSE
Windows Server 2003
Active Directory-Infrastruktur

Die komplette Vorbereitung für das
Examen 70-294

ADDISON-WESLEY

An imprint of Pearson Education

2

Bereitstellen des DNS-Servers für das Active Directory

Lernziele

In diesem Kapitel lernen Sie alle Aspekte eines DNS-Servers kennen, die die Planung und Ausführung eines Active Directory betreffen. Es beginnt mit allgemeinen Grundlagen und endet mit der Darstellung von speziellen Einstellungen für das und mit dem Active Directory. Informaonen über den DNS-Server im Allgemeinen finden Sie auch im MSCE-Kursbuch »*Windows Server 2003-Netzwerkinfrastruktur*«, der ebenfalls im Addison-Wesley-Verlag erschienen ist.

Dieses Kapitel richtet sich nicht nur an den Anfänger, sondern auch an Fortgeschrittene, die ereits Kenntnisse in der Planung und Wartung der Active Directory Services besitzen. Blättern Sie daher später immer einmal zu diesem Kapitel zurück. Es lohnt sich!

olgende Themen werden behandelt:

- Planung einer DNS-Infrastruktur mit DNS-Servern von Microsoft und anderen Herstellern
- Aufgaben und Rollen eines DNS-Servers
- Der Zusammenhang zwischen dem Namensraum und Active Directory-Domänen
- Verfahren zur Integration von DNS-Zonen in das Active Directory und Konsequenzen dieses Vorgangs.

Lernstrategien

Kapitel 2 ist so gestaltet, dass es beim erneuten Durchlesen »aus einem Guss« ist. Für den Anfang, wenn das Thema noch völlig neu sein sollte, sind folgende Schritte empfehlenswert:

- Falls das Thema Domain Name System (DNS) für Sie neu ist, beginnen Sie mit *Kapitel 2.1* und lesen Sie bis zum Endes dieses Kapitels. Falls Sie noch Fragen zum DNS haben, empfehlen wir Ihnen weiterführende Literatur.
- Anschließend installieren Sie einen Domänencontroller (siehe *Kapitel 3*) und rekonstruieren die Rolle des DNS. Dies wird in den *Kapiteln 2.2 bis 2.2.5* beschrieben. Sie sind anschließend in der Lage, die nachfolgend gezeigten Übungen auszuführen.
- Es kann durchaus sein – und das ist bewusst so eingerichtet –, dass Sie nach dem Durcharbeiten der *Kapitel 3 und 4* nochmals zu *Kapitel 2* zurückkehren, in der Absicht, die verschiedenen Dienste und Rollen eines Domänencontrollers in der DNS-Zonendatenbank zu reflektieren. Sie sollten dann die *Kapitel 2.2.6 bis Ende 2.3* wiederholend behandeln.

Kapitel	Zielgruppe/Zweck
Kapitel 2.1	Einsteiger/Vertiefen des Stoffs
Kapitel 2.2 bis Kapitel 2.2.5	Für Fortgeschrittene, die schon einmal einen Domänencontroller mit DNS-Server installiert haben
Kapitel 2.2.6 bis Ende	Für Fortgeschrittene, die Kenntnisse in der Funktionsweise des Active Directory besitzen

Tabelle 2.1: *Kapitelunterteilung*

Die Planung und Einrichtung der DNS-Infrastruktur ist in der Prüfung 70-294 kein primäres Thema. Es kann allerdings sein, dass Sie im Rahmen des Themenblocks *Planen und Implementieren einer Active Directory-Infrastruktur* die eine oder andere Frage erhalten, die dieses Thema streift.

2.1 Planen einer DNS-Infrastruktur

Das Planen der DNS-Namensauflösung legt den Grundstock für die Einrichtung des Active Directory. Da dem Domain Name System eine große Bedeutung zukommt (denn ohne würde kein Active Directory laufen), werden nachfolgend nicht nur spezielle Einstellungen, sondern auch Grundlagen vermittelt.

2.1.1 Begriffe und Definitionen

Die folgenden Begriffe und Definitionen spielen bei der Verwendung von DNS eine Rolle. Viele Begriffe kommen aus dem Englischen und eine schlüssige Übersetzungsstrategie manchmal nicht erkennbar. Da Begriffe und Definitionen für die MCSE-Prüfungen wichtig

Begriff	Definition
Autorisierender Namenserver	Ein DNS-Server, der Abfragen nach DNS-Namen beantworten kann. Er hat somit die Autorität, DNS-Abfragen für eine bestimmte Zone aufzulösen. Ein autorisierender Namenserver hostet eine lokale Zonendatei oder ist in Active Directory integriert.
Bedingte Weiterleitung	Kann ein autorisierender Namenserver die DNS-Anfrage eines DNS-Clients nicht beantworten, wird eine Weiterleitung initiiert. Bei der bedingten Weiterleitung wird mit der Weiterleitung eine Bedingung an die Weiterleitung verknüpft. Die Weiterleitung übergibt die Abfrage nun an einen DNS-Server in der angegebenen Domäne. DNS-Server, die für die bedingte Weiterleitung konfiguriert sind, müssen zur Namensauflösung nicht auf die Rekursion zurückgreifen.
BIND-Server	Ein leistungsfähiger DNS-Namenserver, der auf einem Linux- oder UNIX-Server ausgeführt wird. BIND ist die Abkürzung für *Berkeley Internet Name Domain*.
Delegierung	DNS-Namensräume können in zusätzliche Zonen aufgesplittet werden. Beim DNS ist die Delegierung die Zuweisung der Verantwortung für eine DNS-Zone. Sie findet statt, wenn ein Ressourceneintrag eines Namenservers in der übergeordneten Zone denjenigen DNS-Server auflistet, der für die untergeordnete Zone autorisierend ist. Der gleiche Vorgang kann auch verwendet werden, um die Verantwortung für Domänennamen zwischen den DNS-Servern im Netzwerk zu verteilen.
DNS-Namensraum	Der DNS-Namensraum ist eine hierarchische baumartige Struktur von Namen. Jeder Name bezeichnet eine Domäne bzw. Zone. Die Schreibweise hierfür ist ein vollqualifizierter Domänenname (Fully Qualified Domain Name, FQDN). Der DNS-Namensraum wird auch als *DNS-Namespace* bezeichnet.
DNS-Resolver	Der DNS-Resolver ist ein Dienst, der auf DNS-Clients ausgeführt wird. Er ist für die DNS-Abfragen an den DNS-Server zuständig.
DNS-Server	Hiermit ist ein Computergerät gemeint, das den DNS-Server-Dienst ausführt. FQDNs werden in IP-Adressen aufgelöst. Als Betriebssysteme kommen Windows NT, Windows 2000 Server oder Windows Server 2003, aber auch andere Betriebssysteme in Betracht.
Externer Namensraum	Ein öffentlicher Namensraum (Namespace) wie das Internet. Der Namensraum wird von der *Internet Corporation for Assigned Names and Numbers* (ICANN) und anderen, wie zum Beispiel DENIC, verwaltet.
Vollqualifizierter Domänenname	Ist die deutsche Übersetzung von *Fully Qualified Domain Name (FQDN)*. Es ist ein Standard, nach dem Zonen, Domänen und Hosts benannt werden. Der FQDN eines Hosts im Internet ist zum Beispiel `www.microsoft.com`.
Interner Namensraum	Der Namensraum (Namespace), der von einer Organisation (Firma, Privatleuten, etc.) genutzt werden kann. Interne Namensräume schirmen den Zugriff vom Internet ab. Eine öffentliche Vergabe existiert nicht.

abelle 2.2: *Wichtige Begriffe für die Verwendung von DNS (alphabetisch geordnet)*

Begriff	Definition
Nameserver/ Namenserver	Ein DNS-Server, der auf DNS-Auflösungsanforderungen von Clients innerhalb einer vordefinierten Zone antwortet. Anmerkung: Bei der Übersetzung des Begriffs ist sich Microsoft selbst nicht schlüssig. In anderen Büchern können Sie auch die Übersetzung *Namensserver* finden. In diesem Werk wird die Übersetzung *Namenserver* verwendet.
Masternamenserver	Ein DNS-Server, der die Kopie seiner Zonendatei anderen sog. sekundären Namenservern (DNS-Servern) zur Verfügung stellt. Ein Masternamenserver kann seinerseits auch ein sekundärer Namenserver sein.
Primärer Namenserver	Der primäre Namenserver hostet die Masterkopie der Ressourcendatenbank. Er ist für die Namensauflösung in derjenigen Zone verantwortlich, für die er die Autorität besitzt. Die Ressourcendatenbank ist in einer lokalen Zonendatei gespeichert, jedoch nicht in einer Active Directory-Datenbank.
Sekundärer Namenserver	Ist ein Server, der eine Kopie der primären Zone von einem primären Namenserver erhält. Die Zonendatei ist nur lesbar, d.h., sie kann nicht beschrieben werden. Sekundäre Namenserver können zur Redundanz und zum Lastenausgleich, aber auch als Masternamenserver verwendet werden.
Ressourceneintrag (Resource Record, RR)	RR-Typen werden in der DNS-Datenbankstruktur verwendet. Ein A-Record enthält beispielsweise einen Hostnamen und eine IP-Adresse.
Stubzone	Eine Teilkopie einer Zone. Mit einer Stubzone und bedingter Weiterleitung lässt sich das Routing des DNS-Datenverkehrs in einem Netz kontrollieren. Eine Stubzone erlaubt einem DNS-Server, Namen und Adressen von zuständigen DNS-Servern zu erkennen, ohne dass der Server mit der Stubzone selbst eine vollständige Kopie der Zone besitzen muss.
Zone	Ein zusammengehöriger Bereich eines Namensraums in einer Ressourcendatenbankdatei. Die Zone enthält die Ressourceneinträge für alle Namen und Dienste innerhalb der Zone. Die Zone kann noch in weitere Domänen unterteilt sein.
Zonenübertragung	Wird eine Zonendatei von einem primären Namenserver auf einen sekundären Namenserver übertragen, heißt der Prozess Zonenübertragung. Die Zonenübertragung findet im Zusammenhang mit der Synchronisation von dem primären- auf sekundäre Namenserver statt.

Tabelle 2.2: *Wichtige Begriffe für die Verwendung von DNS (alphabetisch geordnet) (Forts.)*

2.1.2 Grundlegende Arbeitsweise von DNS

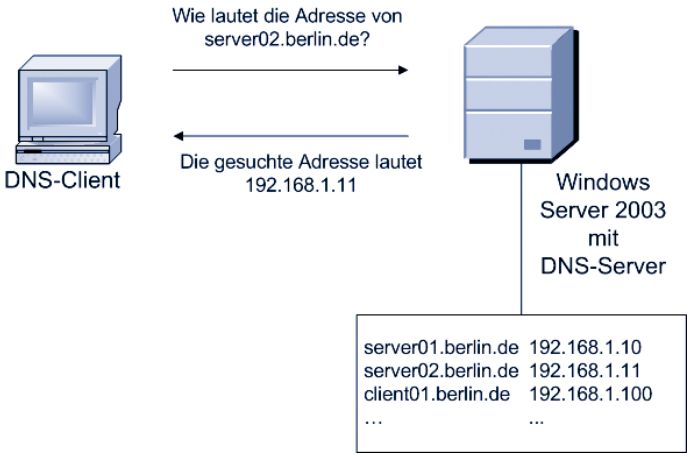
Das *Domain Name System* (DNS) ist ein Standardnamensdienst für IP-basierte Netzwerke, wie das Internet. Das Domain Name System dient zur Benennung von Computern und Netzwerkdiensten (zum Beispiel Mail-Exchanger) in einer hierarchischen Domänenstruktur. Statt den Computern »komplizierte« Internetadressen zu geben, verwendet man einen benutzerfreundlichen DNS-Namen. Dieser Name soll einprägsam sein und gleichzeitig den Standort des Computers (Hosts) anzeigen. Da jedoch die Computer nicht mit ihren Namen über das Netzwerk miteinander kommunizieren, benötigen diese die IP-Adresse des jeweili-

gen Kommunikationspartners. Es muss also immer eine Zuordnung des Namens zu seiner P-Adresse existieren. Dies kann in einer Datenbank erfolgen. Für die Auflösung der Namen existieren zwei Lösungen:

. Einsatz einer statischen Datenbank in Form einer Tabelle: Namensauflösung über die Hosts-Datei. Die Pflege der Datenbank erfolgt manuell.

. Einsatz eines Dienstes, der die Informationen der Datenbank dynamisch pflegt. Hier existiert für Microsoft-Netzwerke der DNS-Dienst und für UNIX/Linux-Systeme der BIND-Server(dienst).

Mit dem DNS-Dienst kann ein Clientcomputer im Netzwerk DNS-Domänennamen registrieren und auflösen. Diese Namen werden für die Suche und für den Zugriff auf Netzwerkressourcen benötigt. In den folgenden Abschnitten finden Sie weitere Informationen zur Namensauflösung.



bbildung 2.1: *Prinzipielle Arbeitsweise eines DNS-Servers: hier die lokale Auflösung einer Adresse*

Domänennamen

Das Domain Name System (DNS) ist ursprünglich in den RFCs (Requests for Comments) 034 und 1035 definiert worden. RFCs werden bei der IETF (Internet Engineering Task orce) eingereicht, die anschließend den Inhalt überprüft, weiterentwickelt und genehmigt. In den o.g. Richtlinien ist die Arbeitsweise von DNS beschrieben. Dort wird ein Domänennamensraum (Namespace) für eine strukturierte Domänenhierarchie vorgeschrieben, nach dem sich zum Beispiel jeder Internetanwender richten muss.

n Ressourceneinträgen werden im DNS die DNS-Domänennamen den Ressourceninformationen zugeordnet. Die Ressourceneinträge dienen letztendlich zum Registrieren oder Auflösen im zugehörigen Namensraum. Die Domänennamen werden von Organisationen wie DENIC Deutschland) oder INTERNIC verwaltet.

Wenn in diesem Zusammenhang von einer Domäne gesprochen wird, ist immer eine Internet-, aber keine Microsoft-Domäne gemeint. Microsoft Domänen haben in Anlehnung an das Internet gleiche Namen und auch eine gleiche Namensstruktur, sie haben aber mit einer Internetdomäne sonst nichts gemeinsam. Eine Domäne fasst hier Computer (Hosts), Aliasnamen und Dienste mit ihren Namen zusammen.

Namensräume

Wie kann man sich in der Praxis einen Namensraum (Namespace) vorstellen? Eine Anlehnung können Sie in dem Organigramm-Prinzip finden. An der Spitze steht ein Stamm, der *Stammdomäne* (Root) genannt wird. Per Definition wird der Stamm mit zwei leeren Anführungszeichen ("") bezeichnet. Bei der Verwendung in einem DNS-Domänennamen wird er durch einen nachgestellten Punkt (.) dargestellt.

Die Stammdomäne ist die höchste Domäne in der Hierarchie.

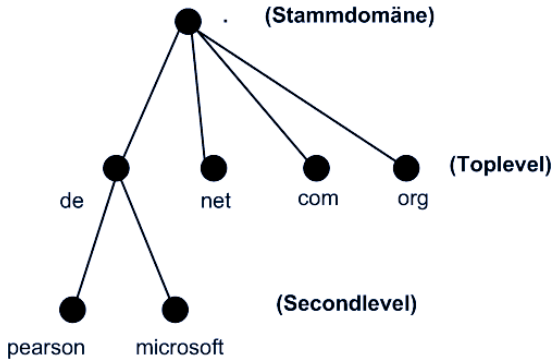


Abbildung 2.2: *Hierarchisch angeordnete Namensräume im Internet*

Die der Stammdomäne direkt untergeordneten Domänen, wie *.com* (ausgesprochen *dot-com*), *.de* usw. sind die sog. *Topleveldomänen*. Idealerweise repräsentieren sie die Länder (*.de* wie Deutschland, *.it* wie Italien etc.), es gibt jedoch auch Topleveldomänen, die Zusammenfassungen von Domänen mit einem öffentlichen Auftrag darstellen. Das ist zum Beispiel bei der Domäne *.org* der Fall. Einige Domänen wurden früher nur innerhalb der USA verwendet, wie beispielsweise *.com* oder *.edu*. Heute kann jedoch jeder Nutzer seine Domäne unter *.com* registrieren lassen.

In der Ebene unter den Topleveldomänen folgen die *Secondleveldomänen*. Hier dürfen beliebige Namen stehen. Lediglich die Syntax ist vorgegeben. So dürfen nach RFC 1123 nur Ziffern von 0 bis 9, Bindestriche und Buchstaben von A bis Z und a bis z (ohne Umlaute) in den Namen vorkommen. Es wird allerdings nicht zwischen Groß- und Kleinschreibung unterschieden. Länderspezifische Buchstaben sind immer ausgenommen. Der Domänenname muss wenigstens einen Buchstaben enthalten. Er darf mit keinem Bindestrich beginnen oder enden. Der Bindestrich darf auch nicht an der dritten oder vierten Stelle eingefügt werden. Die Mindestlänge

dass die Namen der anderen Topleveldomänen nicht als Secondleveldomänen verwendet werden dürfen. Auch ist die Verwendung von deutschen Kfz-Kennzeichen unzulässig. Je nach Gesetzeslage können die Bestimmungen in den verschiedenen Ländern unterschiedlich sein.

eachten Sie, dass für Windows Server 2003 erweiterte Namensregeln, wie vergleichsweise m Internet (RFC 1123), gelten. Windows-Server ab der Version 2000 haben diesen erweiterten Standard, der wiederum nicht mit dem Standard im Internet kompatibel ist.

Zeichensatz-einschränkung	Standardmäßiges DNS (einschließlich Windows NT 4.0)	DNS unter Windows 2000 und Windows Server 2003
Zulässige Zeichen	Unterstützt RFC 1123. Der Name darf enthalten: Buchstaben A-Z Buchstaben a-z Ziffern 0-9 Bindestrich -	Unterstützt RFC 1123 und UTF-8 (RFC 2044). UTF-8 ist eine Obermenge von ASCII und eine Übersetzung der UCS-2-(oder Unicode-)Zeichencodierung. Der UTF-8-Zeichensatz kann nur in Windows 2000- oder Windows Server 2003-Umgebungen eingesetzt werden.
Maximale Länge für Hostname und FQDN	63 Zeichen (1 Zeichen = 1 Oktett) pro Bezeichnung. 255 Byte pro FQDN (254 Byte für den FQDN plus ein Byte für den abschließenden Punkt).	Entspricht dem standardmäßigen DNS (63 Zeichen) plus der UTF-8-Unterstützung Einige UTF-8-Zeichen überschreiten die Länge von einem Oktett. Domänencontroller sind auf 155 Byte für einen FQDN beschränkt.

abelle 2.3: *Vergleich von DNS unter Windows NT und unter Windows 2000/2003*

eispiele für Secondleveldomänennamen sind *pearson.de* oder *microsoft.de*. Jeder Domänenname darf genau einmal im Internet vorkommen. Seine Eindeutigkeit muss immer gewahrt werden.

TIPP

Sie können den DNS-Namen aus Ihrem Internetauftritt auch für Ihre Microsoft-Domäne verwenden. Besser ist es jedoch, wenn Sie beide Namensräume voneinander trennen: einen Namensraum für den Internetauftritt und einen für den internen Gebrauch. Achten Sie bei der Planung der Active Directory-Struktur auf diese Konformität des DNS-Namens zum Active Directory-Domänennamen.

Vollqualifizierte Domänennamen

DNS-Domänennamen werden auch oft als *vollqualifizierte Domänennamen* bezeichnet. Auch das englische Kürzel für *Fully Qualified Domain Name* (FQDN) ist gebräuchlich.

Wie in dem vorangegangenen Unterkapitel schon erläutert wurde, bestehen Namensräume aus hierarchisch angeordneten Domänennamen. Platziert man nun einen Computer (Host) mit einer Netzwerkkarte in diesen Namensraum, bekommt die Netzwerkkarte eine IP-Adresse nd einen FQDN. Dieser FQDN ist von der IP-Adresse und deren Klassifizierung in einem der

Der resultierende Domänenname besteht aus dem Namen der Topleveldomäne (erste Ebene), dem Namen der Secondleveldomäne (zweite Ebene) und weiteren untergeordneten Domänennamen. Die Namen sind jeweils durch einen Punkt getrennt. Der fortlaufende Name ist von rechts nach links angeordnet.

Formal gesehen ist die Regel mit

```
(Domäne N).(Domäne N-1).   ...   (Domäne 1)
```

zu beschreiben.

Für einen Hostnamen, d.h. einen Computernamen, oder einen Aliasnamen gilt, dass dieser immer ein Präfix vor dem letzten (untergeordneten) Domänenbezeichner ist.

```
Hostname.(Domäne N).(Domäne N-1).   ...   (Domäne 1)
```

In dem oben genannten Beispiel ist der FQDN für Microsoft:

```
microsoft.de
```

Ein Computer, der sich in dieser Domäne befindet, hat den folgenden Namen:

```
hostname.microsoft.de
```

Aliasnamen

Aliasnamen sind zusätzliche Namenseinträge für einen Host. So kann man einem Host, d.h. einer IP-Adresse, mehrere Aliasnamen zuweisen. Fragt ein DNS-Client nach den Aliasnamen, bekommt er von seinem DNS-Server die zugehörige IP-Adresse geliefert. Anschließend kann er über die IP-Adresse auf den gewünschten Host zugreifen. Aliasnamen werden im Internet gerne mit »WWW« gekennzeichnet. Andere Aliasnamen sind jedoch auch zulässig. Sie müssen den Bestimmungen des jeweiligen Landes und den allgemeinen Bestimmungen zur Namensvergabe genügen.

Ein Beispiel für einen FQDN ist *www.pearson.de*. Von einem DNS-Client aus, ist es nicht ersichtlich, welcher der eigentliche Name und welcher der Aliasname eines Hosts ist.

Zonen

Das Domain Name System erlaubt eine Unterteilung des Namensraums in Zonen. In einer Zone sind eine oder mehrere Namensinformationen zusammengefasst. Die Zone ist die autorisierende Quelle aller Informationen für alle in ihr enthaltenen DNS-Domänennamen. Jede Zone muss einen zusammenhängenden DNS-Namensraum haben. Die Verknüpfungen zwischen den Host-Namen und den IP-Adressen werden normalerweise für jede Zone in einer Zonendatenbankdatei gespeichert. Die Zone beginnt mit der Speicherung der ersten Domäne (siehe auch *Abbildung 2.3*). Wo liegt nun der Unterschied zwischen Zone und Domäne? In den meisten Fällen ist der Name der Zone mit dem der Domäne identisch. Eine Zone benötigt jedoch immer eine Zonendatei, um Ihre Domänennamen und andere Informationen abzuspeichern.

Falls Sie Microsoft Active Directory verwenden, können Sie anstelle der Zonendatenbankdatei

ür jede Zone gibt es eine fest verbundene Domäne, die als *Stammdomäne* der Zone bezeichnet wird. In der Stammdomäne befinden sich nur die Informationen zu ihren Subdomänen. Die Namen werden nach folgender Regel zusammengefasst:

```
Hostname.(Zone Z).(Zone Z-1). ... (Zone 1)
```

Eine Mischung aus Zonen- und Domänenbezeichnern ist ebenfalls möglich.

```
Hostname.(Domänenname N).(Zone Z).(Zone Z-1). ... (Zone 1).(Domänenname 1)
```

Hierbei sind N und Z ganze natürliche Zahlen.

Wie Sie aus den beiden Definitionen ersehen können, gibt es im Ergebnis keinen Unterschied wischen Zonen und Domänen. Es gibt zwei Arten von DNS-Zonen:

- Forward-Lookupzonen und die
- Reverse-Lookupzonen.

HINWEIS

Wenn Sie den Microsoft DNS-Server verwenden, müssen Sie zuerst eine *Forward-Lookupzone* einrichten. Anschließend können Sie innerhalb der Zone untergeordnete Domänen einrichten.

Zusammenfassung zweier Domänen zu einer Zone

In der nebenstehenden Zeichnung erkennen Sie, dass die Domänen

- pearson-zentrale.de
- addison-wesley.pearson-zentrale.de
- muenchen.addison-wesley.pearson-zentrale.de

zu einer Zone mit dem Namen *pearson.de* zusammengefasst werden.

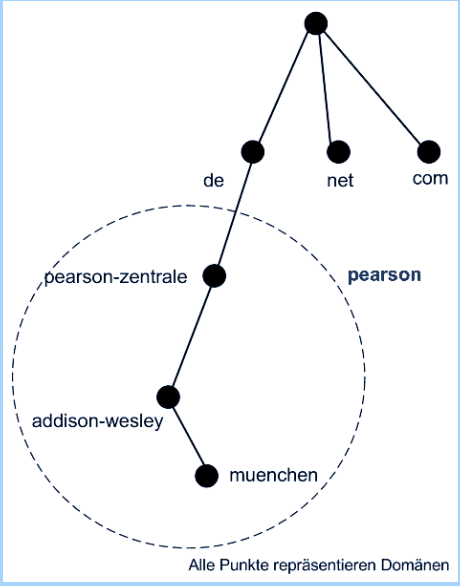


Abbildung 2.3: *Zusammenfassen von drei Domänen zu einer Zone*

Forward- und Reverse-Lookupzonen

Bei den meisten DNS-Vorgängen handelt es sich um Forward-Lookups. Ein DNS-Client erwartet von einem DNS-Server die IP-Adresse eines Hosts, die der Host zwecks Kommunikation erreichen will. Für diesen Vorgang hat der DNS-Server in einer Forward-Lookupzone einen Eintrag gespeichert. Darin ist der DNS-Name der IP-Adresse zugeordnet. Alle Einträge sind in der Zonendatenbankdatei abgelegt. Der Eintrag des Hosts in diese Datei wird als *Adressressourceneintrag* (A) bezeichnet und ist in dem RFC 1035 definiert.

```
Asterix         A     192.168.1.10
Idefix          A     192.168.1.11
Obelix          A     192.168.9.200
```

Listing 2.1: *Auszug aus der Zonendatei (Beispiel) eines DNS-Servers im lokalen Netzwerk*

Aus dem oben gezeigten Listing ist zu ersehen, dass die Abfrage nach einer IP-Adresse einfach ist, zumal es sich um einen Computer im lokalen Netzwerk handelt. Möchte der DNS-Client einen Internethost erreichen, kann sein DNS-Server so eingestellt werden, dass dieser an seiner Stelle einen DNS-Server im Internet anfragt. Bei ca. 3,7 Mrd. möglichen Internethosts würde eine Abfrage lange dauern, wenn es nicht leistungsstarke DNS-Server im Internet gäbe, die möglichst alle Internetadressen »cachen«.

In einigen Fällen benötigt der DNS-Client den DNS-Namen eines Kommunikationspartners. Da er die IP-Adresse von diesem kennt, kann er über eine Reverse-Lookupzone den gewünschten Namen geliefert bekommen. Diese Abfrage können Sie sich vereinfacht als folgende Anfrage des Clients vorstellen: »Wie lautet der DNS-Name von dem Computer mit der IP-Adresse 194.128.11.34?«

Da das DNS ursprünglich nicht für die Unterstützung dieses Abfragetyps konzipiert wurde, musste dieser Typ der Abfrage noch in den DNS-Server integriert werden. Das Problem bei der Unterstützung liegt in der umgekehrten Abfrage. Daher wurde hierfür eine spezielle Domäne eingerichtet: die *in-addr.arpa*. Wird nun ein umgekehrter Namensraum abgebildet, werden in der *in-addr.arpa*-Domäne IP-Adress-Oktettzahlen in umgekehrter Reihenfolge der normalen dezimalen Notation verwendet. Diese neue Schreibweise ist erforderlich, weil IP-Adressen von links nach rechts gelesen werden. Für die *in-addr.arpa*-Domänenstruktur ist ein neuer Ressourceneintragstyp erforderlich, der Ressourceneintrag *PTR* (Pointer Ressource).

Für das Subnetz 192.168.0.0/24 soll beispielsweise eine Reverse-Lookupzone eingerichtet werden. Die Zone bekommt nach o.g. Definition den Namen *0.168.192.in-addr.arpa.dns*. Die erste Null, die eigentlich am Anfang stehen müsste, wird nicht angezeigt, da die Subnetzmaske 255.255.255.0 ist. Würde man die Subnetzmaske umdrehen, käme hier 0.255.255.255 heraus. Ein Host in dieser Zone hätte dann den FQDN *168.0.11.0.168.192.in-addr.arpa*. Lautet das Subnetz dagegen 10.0.0.0/8, so heißt die Zone *0.0.10.in-addr.arpa.dns*.

Reverse-Lookupzonen werden im RFC 2317 (»klassenlose« Reverse-Lookupzone) ausführlich erläutert. Zusätzliche Informationen zu IPv6 und DNS finden Sie im RFC 1886.

Stubzonen

Eine Stubzone erlaubt einem DNS-Server, Namen und Adressen von zuständigen DNS-Servern zu erkennen, ohne dass der Server mit der Stubzone selbst eine vollständige Kopie der Zone eines übergeordneten Namenservers besitzen muss. Eine Stubzone ist nur auf Windows Server 2003-basierten DNS-Servern verfügbar.

Eine *Stubzone* ist die Kopie einer Zone, die nur folgende Einträge enthält:

- Autoritätsursprungs-Ressourceneintrag (Start-of-Authority, SOA)
- Namenserver-Ressourceneinträge (NS)
- Ressourceneinträge des Typs A (auch Glue-A-Ressourceneinträge genannt) für die delegierte Zone

Derjenige DNS-Server, der die Stubzone hostet, wird mit der IP-Adresse des autorisierenden DNS-Servers konfiguriert. Von diesem wird die Zone geladen bzw. kopiert. Wenn der DNS-Server mit der Stubzone eine Abfrage nach einem Computernamen derjenigen Zone erhält, auf die die Stubzone verweist, verwendet der DNS-Server die IP-Adresse zum Abfragen des utorisierenden Servers. Andernfalls gibt er bei iterativen Abfragen einen Verweis auf die DNS-Server zurück, die in der Stubzone aufgelistet werden. Genau wie eine normale Zone ann eine Stubzone für rekursive und iterative Abfragen verwendet werden.

Aktualisierungen können Sie in den Einstellungen der jeweiligen Stubzone vornehmen. Sie verwenden die Stubzone für die Weitergabe von Informationen über untergeordnete Zonen, die eine übergeordnete Zone automatisch erhalten soll. Fügen Sie hierzu die Stubzone dem DNS-Server hinzu, der die übergeordnete Zone hostet. Sie können eine Stubzone auch für die Weiergabe von Namensräumen verwenden, obwohl die bedingte Weiterleitung die bevorzugte Methode für diesen Vorgang ist.

Sie können Stubzonen entweder auf die herkömmliche Art dateibasiert speichern oder in das Active Directory integrieren. In diesem Fall muss der DNS-Server auf einem Domänencontroller sein.

Fallstudie: Stubzone

Situationsbeschreibung

Ein DNS-Server1 hostet die Zone *it-consult.de,* und ein DNS-Server2 hostet die Zone *berlin.it-consult.de.* Die Zone *it-consult.de* ist die übergeordnete Zone mit dem autorisierenden DNS-Server1. Dieser soll die untergeordnete Domäne *berlin.it-consult.de* an verschiedene DNS-Server delegieren. Als die Delegierung für die Domäne *berlin.it-consult.de* ursprünglich vorgenommen wurde, enthielt die übergeordnete Zone lediglich Einträge für Namenserver (NS-Einträge) für die autorisierenden DNS-Server der untergeordneten Zone. Später hat man für die untergeordnete Zone weitere autorisierende DNS-Server konfiguriert, jedoch ohne Wissen der Administratoren der übergeordneten Zone.

Folglich kann der DNS-Server, der die übergeordnete Zone hostet die neuen, in der untergeordneten Zone befindlichen autorisierenden Server nicht kennen. Er fragt weiterhin seine bereits bekannten DNS-Server in dieser Zone ab.

Wie können Sie erreichen, dass auch diese Namenserver abgefragt werden können?

Situationsanalyse

Eine Lösung des Problems kann darin bestehen, dass Sie den für die übergeordnete Zone autorisierenden DNS-Server so konfigurieren, dass er die Stubzone für die delegierte Domäne hostet. Mit anderen Worten: Der DNS-Server von *it-consult.de* hostet zusätzlich eine Teilkopie von *berlin.it-consult.de*. Die Stubzone bietet den Vorteil, dass der für die Delegierung »unnütze Ballast« von Service Ressource Records, Mail-Exchanger, usw. nicht auf den DNS-Server1 überspielt wird.

Wenn Sie als Administrator von DNS-Server1 ihre Stubzone aktualisieren, fragt der DNS-Server1 den DNS-Server2 nach Ressourceneinträgen des autorisierenden DNS-Servers für *berlin.it-consult.de* ab (siehe *Abbildung 2.4*). Nachdem die Informationen übertragen worden sind bzw. die Stubzone aufgefüllt worden ist, kann der für die übergeordnete Zone autorisierende DNS-Server über die neuen, für die untergeordnete Zone autorisierenden DNS-Server informiert werden. Die Folge ist, dass alle Namenserver von `berlin.it-consult.de` bei rekursiven Anfragen fremder (übergeordneter) Server eine Namenauflösung leisten können.

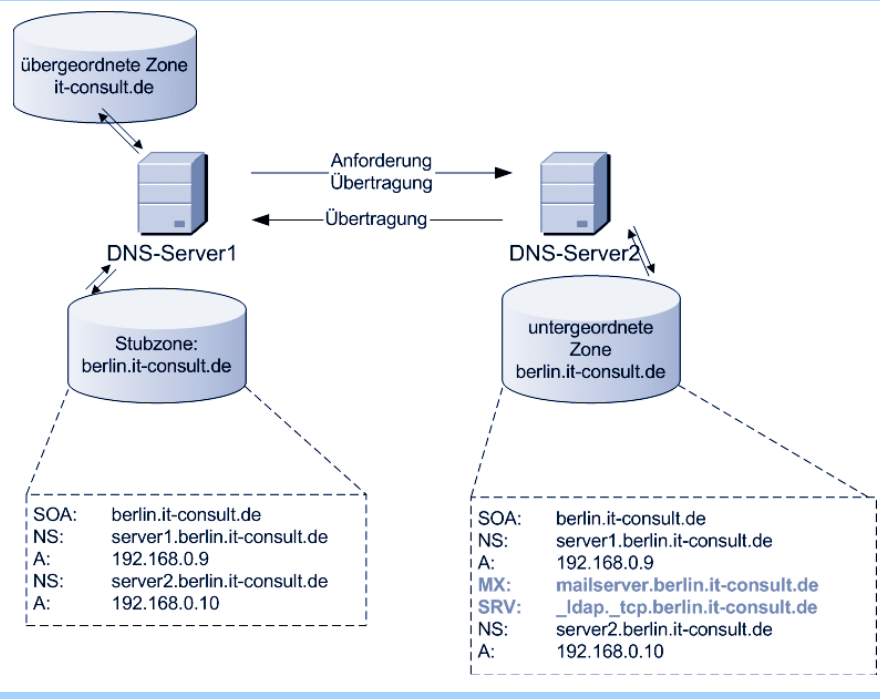


Abbildung 2.4: *Anwenden einer Stubzone*

Zonenübertragungen

Es wurde in diesem Kapitel bereits erwähnt, dass das Domain Name System das Unterteilen des Namensraums in Zonen ermöglicht, in denen die Namensinformationen zu mindestens iner DNS-Domäne gespeichert werden. Für jeden in einer Zone vorhandenen DNS-Namen zw. DNS-Client wird die Zone zur autorisierenden Quelle für die Informationen über diese Domäne.

Wegen der wichtigen Rolle der DNS-Server sollten Sie nach Möglichkeit Zonen fehlertolerant uf mehreren DNS-Servern gleichzeitig ausführen. Bei Fehlfunktionen können Abfragen für Namen und Dienste in der Zone fehlschlagen, wenn nur ein einzelner Server verwendet wird und dieser nicht antwortet. Verwenden Sie die Active Directory Services, dann ist die Verfügbarkeit von DNS Ihr oberstes Gebot. Zu der Rolle von DNS in Active Directory finden Sie weiere Informationen im *Kapitel 2.2.3*.

ei mehreren DNS-Servern, die für eine Zone zuständig sind, müssen alle Informationen der Zone aktualisiert auf den jeweiligen Servern vorliegen. Für die Replikation und Synchronisaon der Zonen ist eine sog. *Zonenübertragung* notwendig.

Um die Fehlertoleranz zu erreichen, gibt es bei Windows-Servern mehrere Möglichkeiten:

. Replikation und Synchronisation einer sekundären Zone. Die sekundäre Zone ist lediglich lesbar, das heißt, es können keine Ressourceneinträge hinzugefügt werden.

. Fehlertoleranz durch Abspeichern der Zoneninformationen in ein Active Directory. Hierbei muss der DNS-Server auch gleichzeitig ein Windows-Domänencontroller sein.

. Zonenübertragungen an fremde DNS-Server. Mit dieser Methode können auch Nicht-Microsoft-DNS-Server, wie BIND-Server, Ressourceneinträge repliziert bekommen.

Damit bei Änderungen in der Zone nicht der vollständige Inhalt der Zone repliziert wird, nterstützt der DNS-Dienst eine inkrementelle Zonenübertragung (IXFR) und einen gegenber Windows 2000 Server überarbeiteten Zonenübertragungsvorgang für vorläufige Ändeungen. Die inkrementellen Zonenübertragungen sind aus dem RFC 1995 entnommen. Sie dienen als zusätzlicher Standard für die Replikation für DNS-Zonen. Es liegt somit auf der Hand, dass Zonenänderungen wesentlich effizienter übertragen werden können. Inkrementelle Zonenübertragungen werden nur von Windows 2000 Server und Windows Server 2003 nterstützt.

Zonenübertragungen können in folgenden Fällen auftreten:

- Die Inhalte der Zone haben sich verändert.
- Nach dem Start des DNS-Serverdienstes auf einem sekundären DNS-Servers (für die entsprechende Zone)
- Nach Ablauf des Aktualisierungsintervalls für die Zone
- Durch manuelles Initiieren einer Übertragung von dem DNS-Server aus, der die sekundäre Zone hostet

Zonenübertragungen auf Windows Server 2003-basierenden Computern werden immer auf

zum DNS-Server mit der Masterkopie der Zone gesendet. Windows-DNS-Server unterstützen nach RFC 1996 eine Benachrichtigung sekundärer Server bei Zonenänderungen.

Aus Sicherheitsgründen lässt der DNS-Server nur Zonenübertragungen an autorisierende DNS-Server zu, die in den Namenserver-Ressourceneinträgen für die Zone aufgelistet sind.

Auflösen eines FQDN

SCHRITT FÜR SCHRITT

DNS-Clients besitzen in den Netzwerkkarteneinstellungen Informationen über ihre DNS-Server. Wenn Sie eine Adresse zum Auflösen eingeben, dann sendet der DNS-Client eine rekursive Anforderung zu seinem bevorzugten DNS-Server. Rekursive Anforderungen verlangen, dass der Remote-Server entweder eine autoritative Antwort oder eine »Nicht gefunden«-Meldung zu dem DNS-Client zurückliefert. Der Rekursionsprozess wird dann aktiviert, wenn keine lokal zwischengespeicherten Daten zum Auflösen der Namensabfrage zur Verfügung stehen.

Der DNS-Server überprüft, ob er die rekursive Anforderung autorisierend beantworten kann. Dies geschieht anhand der Ressourceneinträge in seiner lokal konfigurierten Zone. Entspricht der Name einem Ressourceneintrag (A-Record), antwortet der Server immer autorisierend, indem er seine eigenen Daten zum Auflösen des abgefragten Namens verwendet.

Stehen für den abgefragten Namen keine Informationen zur Verfügung, überprüft der DNS-Server, ob er den Namen mit Hilfe seines Caches auflösen kann. Im Cache sind die zwischengespeicherten Ressourceneinträge aus vorherigen Abfragen abgelegt. Wird eine Entsprechung gefunden, beendet der Server seine Suche und gibt diese Informationen an den DNS-Client weiter.

Wird weder im Cache noch in den Zonendateien des DNS-Servers eine Antwort auf die DNS-Anfrage gefunden, kann der Abfragevorgang nur dann fortgesetzt werden, wenn weitere DNS-Server zur Abfrage bereitstehen. Auch jetzt wird der Rekursionsprozess noch weitergeführt.

Für eine Rekursion benötigt der DNS-Server unterstützende Kontaktinformationen von anderen DNS-Servern. Diese Informationen stehen in Form von Stammhinweisen zur Verfügung. Mit diesen Ressourceneinträgen ist er nun in der Lage, Stammserver zu finden. Die Stammserver sind autorisierend für den Domänenstamm und die Domänen der obersten Ebene des gesamten Namensraums. Einer Abfrage eines Stammservers steht nun nichts im Wege.

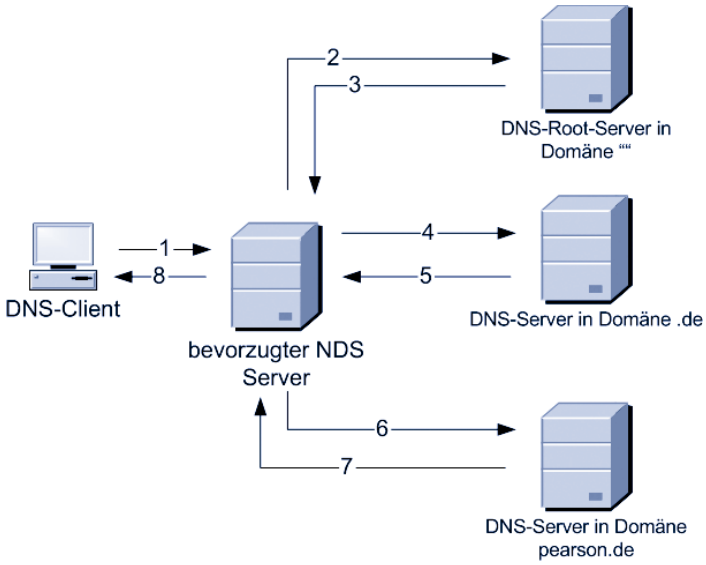
1. Der DNS-Client sendet eine rekursive Anforderung an seinen bevorzugten DNS-Server. Die Anfrage bezieht sich auf einen Host in einer fremden Domäne, hier in der Domäne *pearson.de*.
2. Zunächst analysiert der bevorzugte DNS-Server den FQDN. Er stellt fest, wie in *Abbildung 2.5* zu sehen ist, dass für die Domäne der obersten gesuchten Ebene (hier *de*) der Standort, bzw. die Adresse des autorisierenden Servers benötigt wird. Hierfür wird eine iterative Anforderung an einen DNS-Server der Stammdomäne gesendet.
3. Der DNS-Server der Stammdomäne antwortet mit der IP-Adresse eines Namenservers der *de*-Domäne.
4. Der DNS-Server wiederholt seine Anfrage (wer ist ...?) an den DNS-Server der *de*-

5 Der DNS-Server sendet die Adresse eines DNS-Servers der gesuchten Domäne.

6 Die Anfrage wird schließlich an den DNS-Server gesendet, der den gesuchten Host als Ressourceneintrag in seiner Zonendatenbankdatei enthält.

7 Der suchende DNS-Server bekommt eine autorisierende Antwort vom DNS-Server der Domäne *pearson.de*.

8 Wenn die autorisierende Antwort vorliegt, sendet der DNS-Server diese an den anfordernden Client weiter und speichert sie gleichzeitig in seinem Cache. Der rekursive Abfrageprozess ist hiermit abgeschlossen.



bbildung 2.5: *Rekursive und iterative Namensauflösung über DNS*

ur Abfrage der DNS-Informationen stehen also zwei Anfragetypen zur Verfügung:

- *Rekursive Anforderungen*: Diese Anforderungen stellt der DNS-Client dem DNS-Server.
- *Iterative Anforderungen*: Diese Anforderungen werden von Ihrem DNS-Server an fremde DNS-Server gesendet. Es können mehrere iterative Anforderungen notwendig sein, um eine autoritative Antwort zu erhalten.

ACHTUNG

Beachten Sie, dass ein autorisierender Namenserver ein Server ist, der über die Autorität zum Auflösen von DNS-Abfragen für eine bestimmte Zone verfügt. Dieser DNS-Server enthält die lokale Zonendatei, die auch Active Directory integriert sein kann, mit den Ressourceneinträgen für die Computer und Dienste innerhalb der Zone. Jede Zone verfügt mindestens über einen autorisierenden Namenserver.

2.1.3 BIND-Server

Microsoft richtet sich nach den meisten RFC-Spezifikationen, und zwar so weit, wie es in das Windows Server- bzw. Active Directory-Betriebssystem hineinpasst. Falls Sie eine UNIX/Windows-Netzwerkumgebung haben, sollten Sie die bestehenden BIND-Server (Berkeley Internet Name Domain Server) unter UNIX oder Linux mit in den Namensraum integrieren.

Die meistgestellte Frage ist die, ob auch BIND-Server als DNS-Server für Microsoft-Domänen verwendet werden können. Die Antwort ist: Sie können. Wenn Sie sich für eine solche Lösung entscheiden, müssen Sie jedoch einige »Kleinigkeiten« beachten...

Vorüberlegungen

Die Namensauflösung über ein Domain Name System und das Ablegen der dienstspezifischen Eigenschaften des Active Directory in eine Zonendatei sind die grundlegendsten Leistungsmerkmale, die ein Namenserver erbringen muss. Bei der Installation von Active Directory können Sie wählen, ob der DNS-Serverdienst als Teil der Installation eingerichtet und konfiguriert werden soll oder nicht.

Bei der manuellen Einrichtung des DNS-Servers verzichten Sie auf die einfachere automatische Methode, auf einem Domänencontroller einen DNS-Server auszuführen. Optimal ist es, wenn Sie zwecks Redundanz in jedem Subnetz zwei DNS-Server laufen haben.

Voreingestellt verwenden Windows Server 2003-DNS-Server bei der Zonenübertragung immer eine schnelle Übertragungsmethode nach dem Prinzip der Datenkomprimierung. Für eine Interoperabilität mit DNS-Servern, die diese Methode nicht unterstützen (wie bei Servern, die mit einer früheren Version als BIND 4.9.4 ausgestattet sind) kann das schnelle Übertragungsformat bei Zonenübertragungen deaktiviert werden. Da mittlerweile BIND-Server mit einer Versionsnummer von 9.x.x (Stand Februar 2004) den aktuellen Stand der Technik darstellen, brauchen Sie diese Übertragungsmethode nicht zu verändern.

Kompatible Server

Folgende BIND-Server können für das Hosten von Active Directory-Zonen verwendet werden:

- BIND Server Version 8.1.2 oder höher
- Empfohlen: DNS-Server, die nicht auf Windows Server 2003 oder Windows 2000 Server basieren, müssen dynamische Updates nach RFC 2136 unterstützen. Die sichere dynamische Aktualisierung basierend auf dem GSS-TSIG-Algorithmus (Transaction Signature oder Transaktionssignatur) geht dagegen noch einen Schritt weiter: Nur Computer, die Mitglied einer Active Directory-Domäne sind, können eine Aktualisierung durchführen.
- Obligatorisch: DNS-Server, die nicht auf Windows Server 2003 oder Windows 2000 Server basieren, müssen SRV-Records (Service Location, SRV) unterstützen. Dieser Ressourceneintrag für die Dienstidentifizierung ist im Internetentwurf »A DNS RR for specifying the location of services (DNS SRV)« beschrieben.
- Windows NT Server stellt ebenfalls einen DNS-Server. Dieser ist bedingt »tauglich«, da er keine dynamischen Aktualisierungen zulässt. Dieser DNS-Servertyp muss manuell ver-

HINWEIS

Obwohl es möglich ist, eine manuelle Zonenerstellung zu verwenden, sollten Sie die Zone nach Möglichkeit mit dem Installationsassistenten von Active Directory einrichten. Dabei wird ein DNS-Server auf einem Microsoft Windows Server 2003-Domänencontroller installiert. Dieses Vorgehen ist nicht nur einfacher, es verhindert auch sicher Konfigurationsfehler.

Die folgende Tabelle zeigt Ihnen die unterschiedlichen Leistungsmerkmale von Windows DNS- und BIND-Servern:

Funktion	Windows Server 2003	Windows 2000	Windows NT 4.0	BIND 9	BIND 8.2	BIND 8.1.2	BIND 4.9.7
Unterstützt SRV-Einträge	**x**	X	x	**x**	x	x	x
Dynamische Aktualisierung	**x**	X		**x**	x	x	
Sichere dynamische Aktualisierung	**x**	x					
Schnelle Zonenübertragung	**x**	x	x	**x**	x	x	x
nkrementelle Zonenübertragung	**x**	x		**x**	x		
WINS-, WINS-R-Einträge	**x**	x	x				
Stubzone	**x**			**x**			
Bedingte Weiterleitung	**x**			**x**			
Erweiterungsmechanismus für DNS (EDNS0)	**x**			**x**			
UTF-8-Zeichencodierung	**x**	x					
Active Directory-ntegrierte Zonen	**x**	x					
Speicherung von Zonen in der Anwendungspartition von Active Directory	**x**						
Ablaufzeit und Aufräumvorgänge bei veralteten Einträgen	**x**	x					

abelle 2.4: *Vergleich von Microsoft DNS-Servern und BIND-Servern*

Microsoft DNS-Server und die Zusammenarbeit mit anderen Servern

Bei einer gemischten DNS-Server-Umgebung empfehlen sich folgende Einstellungen:

- Vorhandene DNS-Server für Stammzonen werden nicht auf andere, neue DNS-Lösungen aktualisiert oder migriert.
- Sie stellen den DNS-Server auf allen notwendigen Windows Server 2003-Systemen zur Verfügung. Idealerweise liegt der DNS-Server auf einem Domänencontroller, damit die Zone Active Directory-integriert eingerichtet werden kann.

Wenn Sie bereits einen DNS-Namensraum (Namespace) besitzen, können Sie eine neue Subdomäne als Stamm der ersten Active Directory-Domäne einsetzen. Der DNS-Serverdienst wird automatisch für die Unterstützung von Active Directory konfiguriert. Die übergeordnete Domäne bekommt die neue Subdomäne zugewiesen.

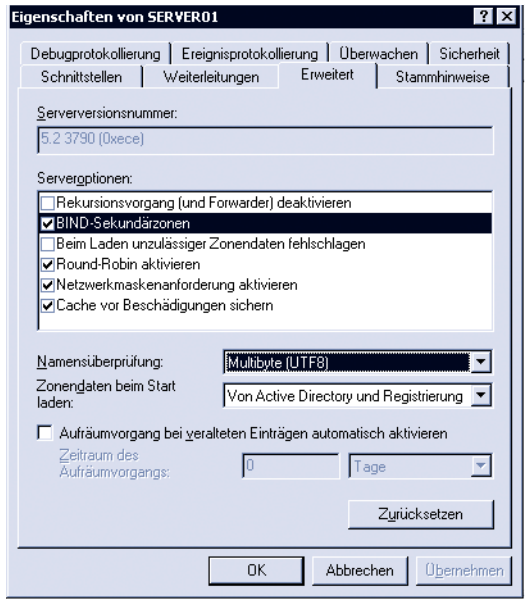


Abbildung 2.6: *BIND-Sekundärzonen und UTF8 werden standardmäßig unterstützt. Diese Einstellungen sind in den Servereigenschaften zu tätigen.*

2.1.4 DNS-Server-Rollen

DNS-Server können verschiedene Rollen einnehmen, um bei großem Anfragevolumen die Leistungsfähigkeit zu vergrößern oder die Ausfallsicherheit zu gewährleisten. Je nachdem, welche Zonendateien der Server hostet, kann man ihm unterschiedliche Rollen zuweisen. Manche DNS-Server teilen sich verschiedene Rollen.

Cache-only-Server und Forwarder

ür einen *Cache-only-Server* müssen Sie lediglich den DNS-Dienst installieren und andere Namenserver angeben, mit denen der Cache-only-Server kommunizieren soll. Wie der Name chon treffend beschreibt, lädt dieser Servertyp nur die Records in seinen Cache. Er hostet eine Zonendatei. Er muss für die rekursiven Anfragen der Clients andere Namenserver (ansonsten macht der Vorgang keinen Sinn) mit einer iterativen Anfrage nach den gesuchten nformationen befragen.

st der DNS-Server als *Forwarder* konfiguriert, kann er andere Server rekursiv befragen. Diese Konstellation ist gerade in großen Netzen bzw. Organisationen sehr sinnvoll, da dort inige wenige DNS-Server die Zonendateien hosten müssen. Die Cache-only-Server dienen ier zum Lastenausgleich.

Primärer Namenserver

Der Begriff *primärer Namenserver* verwirrt ein wenig. Es handelt sich um einen DNS-Server, der eine Zonendatei hostet. Dieser Namenserver ist der Standard. Die Zonendatei liegt im Original vor, d.h., es ist keine schreibgeschützte Kopie.

Ein DNS-Server, der eine Zonendatei hostet, ist in der Lage, schreibgeschützte Kopien an DNS-Server zu senden, die sekundäre Zonen hosten.

ei den primären Namenservern gibt es zwei Untergruppen:

- DNS-Server, die Forward-Lookupzonen hosten
- DNS-Server, die Reverse-Lookupzonen hosten

Sekundärer Namenserver

Hiermit ist ein DNS-Server gemeint, der eine sekundäre Zone hostet. Die sekundäre Zone ist ediglich die Kopie einer primären Zone. Im Gegensatz zu Cache-only-Servern, kann bei ekundären Zonen eine Ausfallsicherheit gewährleistet werden. Ebenso können sie dem Lastenausgleich dienen.

Sekundäre Zonen können nicht in Active Directory gespeichert werden, da Active Directory solch einen Typ nicht vorsieht.

2.2 Der Windows Server 2003-DNS-Bereitstellungsprozess

Um Ihnen den Bereitstellungsprozess zu erleichtern, finden Sie nachfolgend eine Auflistung mit den wichtigsten Designschritten.

1 Überprüfen der Netzwerkinfrastruktur (Netzwerktopologie, Internetanbindung, etc.)

3 Bestimmen der DNS-Namenserver

4 Design der DNS-Zonen

5 Konfigurieren und Verwalten der DNS-Clients

6 Sichern der DNS-Infrastruktur

7 Integrieren in andere Windows Server System-Applikationen

2.2.1 Überprüfen der Netzwerkinfrastruktur

Eine Überprüfung der Netzwerkinfrastruktur beinhaltet nicht nur die Frage, wer die DNS-Server verwalten darf und wo sie stehen, sondern auch, wie bestehende Domänen in eine Microsoft Windows-Domäne eingebaut werden können.

Der Internetauftritt

Einige wenige Firmen (IBM, General Electrics usw.) sind seit Beginn des Internets dabei und haben ihr Netzwerk für ihre Zwecke auch im Internet registrieren und damit reservieren lassen. Alle anderen Nutzer können nur einzelne IP-Adressen oder Subnetze registrieren lassen. Für diese IP-Adressen, die ja über den Bereich des lokalen internen Netzwerks hinaus gehen, benötigen Sie für die Namensauflösung einen DNS-Domänennamen und IP-Adressen in Zonendateien auf DNS-Servern im Internet. Als DNS-Server sind zurzeit überwiegend BIND-Server im Einsatz.

Die Internetregistrierungsstellen, die Ihren Internetauftritt verwalten, stellen Ihnen folgende Dienstleistung zur Verfügung:

- Zuweisen von IP-Adressen
- Registrieren von DNS-Domänennamen
- Anlegen von öffentlichen Einträgen mit registrierten IP-Adressen und Domänennamen

Haben Sie ein lokales Netzwerk, das nicht mit dem Internet verbunden ist, können Sie theoretisch jeden möglichen IP-Adressbereich selbst auswählen. Beachten Sie jedoch, dass es beim Anschluss zum Internet große Probleme geben kann, wenn Sie intern auch öffentliche IP-Adressen verwenden. Router können somit jeden Punkt in und aus dem Netz anwählen. Wenn Sie für Ihr internes Netz einen privaten IP-Adressbereich verwenden, vermeiden Sie Sicherheitslücken.

Ein wesentlicher Planungsaspekt stellt sich mit der Frage, wer die DNS-Daten hosten soll. Wollen Sie diese selbst hosten, oder beauftragen Sie Ihren Internetdienstleister (Internet Service Provider, ISP)? Beide Aspekte haben Vor- und Nachteile, und Sie müssen entscheiden, worauf Sie mehr Gewicht legen: Beim »Selberhosten« steuern Sie selbst alle Einträge und haben eine bessere Bandbreitenausnutzung Ihrer Internetleitung. Geben Sie dagegen das Hosten an Ihren ISP ab, sparen Sie Arbeit und müssen keinen extra DNS-Server (Lizenz- und Hardwarekosten) vorhalten. Haben Sie das Know-how, dann können Sie auch einen BIND-Server neuerer Version unter Linux kostengünstig einrichten. Diese Konstellation ist

Der DNS-Name

Seltsamerweise sind es bei vielen Projekten – sei eine Migration, sei es eine Neukonzeptionieung – gerade die einfachen Themen, die zu kontroversen Debatten innerhalb der Führungstage und allen Beteiligten führen.

inden Sie einen Namensraum für alle Domänen, mit dem die eigene Belegschaft und auch nternationale Partner etwas anfangen können. Schön ist es immer, wenn sich die Firma und deren Philosophie im DNS-Domänennamensraum widerspiegelt. Hat man den Namen gefunden, kann dieser für Microsoft Active Directory-Domänen verwendet werden.

olgende Richtlinien helfen Ihnen bei der Namensgebung:

- Wählen Sie leicht einprägsame und eindeutige Computernamen aus.
- Clientcomputer können den Namen des Anwenders bekommen.
- Servergeräte können Namen bekommen, die den Zweck beschreiben.
- Unterscheiden Sie nicht zwischen Groß- und Kleinschreibung.
- Verwenden Sie den Active Directory-Domänennamen für das primäre DNS-Suffix des Computernamens.
- Verwenden Sie die Internetrichtlinien nach RFC 1123, indem Sie nur ASCII-Zeichen verwenden, sofern Sie nicht Windows 2000 Server oder Windows Server 2003 verwenden.

Die Dokumentation

Zeichnen Sie den Ist-Stand vor der Aktualisierung auf Windows Server 2003 auf. Dokumenieren Sie alle Änderungen im Migrationsprojekt. Haben Sie nur eine Domäne, ist dies schnell erledigt; bei 30 Domänen beispielsweise ist die Dokumentation etwas aufwändiger und allein wegen der Größe schon ein Muss.

2.2.2 Design eines DNS-Namensraums

Vor der Bereitstellung einer DNS-Infrastruktur müssen Sie einen DNS-Namensraum entwerfen. Die folgenden Aspekte sollten Sie beachten:

- Anforderungen an den DNS-Namensraum
- Interne und externe Domänen?
- Entscheiden Sie, ob Sie einen internen DNS-Root benötigen.
- Namensauflösung für mehrere Topleveldomänen notwendig?
- Integrieren Sie Windows Server 2003-DNS in eine bestehende DNS-Struktur?
- Erstellen Sie Subdomänen?
- Konsolidieren Sie DNS-Namensräume?

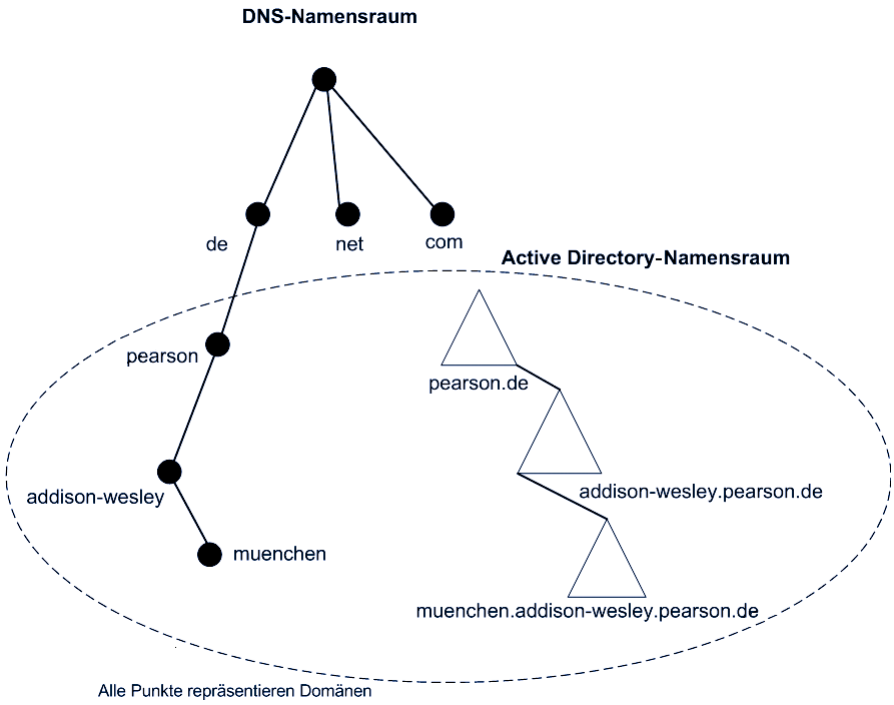
Anforderungen an den DNS-Namensraum: Der Zusammenhang zwischen DNS und Active Directory

Der erste Schritt bei der Planung des DNS-Namensraums ist die Entscheidung, ob ein neuer Namensraum notwendig ist oder nicht. Im letzteren Fall behalten Sie den vorhandenen Namensraum.

Ein Namensraum ist eine hierarchisch gegliederte Namensstruktur, in der Namen in einer Art von Bereichen so zusammengefasst sind, dass die Zugehörigkeit eines benannten Objekts zu dem Bereich einfach herausgefunden werden kann. DNS-Domänen und Active Directory-Namensräume können die gleiche Namenskonvention (Erweiterung durch UTF-8) und eine identische Namensstruktur verwenden. Die Folge ist, dass DNS-Knoten und Active Directory-Domänen gleichermaßen präsentiert werden können.

In einem DNS-Namensraum speichern Zonen alle Informationen über Namen und Dienste von einer oder mehreren Domänen. Die Zone ist ein zusammengehöriger Bereich eines Namensraums in einer Ressourcendatenbankdatei in einem DNS-Namenserver. Anhand der Zoneninformationen kann der DNS-Server Abfragen, wie die nach DNS-Namen, beantworten. Er hat somit die Autorität, diese DNS-Abfragen für die bestimmte Zone aufzulösen. Ein autorisierender Namenserver hostet immer eine lokale Zonendatei oder ist Active Directory-integriert.

Beachten Sie, dass sich zwar Active Directory und Internet die gleiche Namenskonvention teilen, dass jedoch eine Internetdomäne nichts mit einer Active Directory-Domäne zu tun hat.



ACHTUNG

Ihre Active Directory-Infrastruktur richtet sich nach dem DNS-Namensraum!

Die folgende Tabelle zeigt Ihnen mögliche Szenarien und eine entsprechende DNS-Lösung:

Szenario	DNS-Lösung
Sie besitzen eine DNS-Infrastruktur für Windows NT oder Windows 2000 Server mit einem Microsoft Exchange Server.	Eine Änderung des DNS-Namensraums ist für Windows Server 20003 Active Directory nicht erforderlich.
Sie besitzen eine korrekt eingerichtete DNS-Infrastruktur für UNIX/Linux. Es wird ein BIND-Server 8.1.2 oder eine aktuellere Version eingesetzt.	Eine Änderung des DNS-Namensraums ist für Windows Server 20003 Active Directory nicht erforderlich. Eine Integration in Windows Server 2003 ist möglich.
hre vorhandene DNS-Software entspricht nicht den standardisierten Richtlinien für DNS-Domänennamen.	Aktualisieren Sie Ihre DNS-Infrastruktur. Wenn Sie vollständig auf eine homogene Windows-Struktur wechseln wollen, können alte DNS-Server später entfernt werden. Richten Sie eine DNS-Infrastruktur nach den Richtlinien für eine Windows Active Directory-Domäne ein.
Sie haben noch kein Netzwerk und wollen eins neu einrichten.	Entwerfen Sie eine logische Namenskonvention für den DNS-Namensraum, die auf den Namenskonventionen für DNS-Domänen beruht.
Sie möchten einen bestehenden Namensraum verändern.	Überprüfen Sie jede Domäne daraufhin, ob der Nutzen den Aufwand rechtfertigt. Eine Konsolidierung ist ein sehr arbeitsaufwändiger Vorgang.

abelle 2.5: *DNS-Namensräume und der Gebrauch mit Windows Server 2003 Active Directory-Domänen.*

Erstellen von internen und externen Domänen

Wenn Sie eine Internetpräsenz benötigen – und das ist heutzutage ein Standard –, müssen Sie owohl einen internen als auch einen externen DNS-Namensraum bereitstellen. Jeden Namensraum müssen Sie separat verwalten. Hierfür haben Sie drei Möglichkeiten:

- Für die interne und die externe Domäne kann der gleiche Name verwendet werden. Diese Methode kann zu Problemen bei der Namensauflösung aufgrund nicht eindeutiger Namen führen. Mit dieser Konfiguration ist die Verwaltung sehr schwierig.
- Für die interne und die externe Domäne können verschiedene Namen verwendet werden. Auch mit dieser Konfiguration ist die Verwaltung nicht einfach.
- Die interne Domäne kann zu einer untergeordneten Domäne der externen Domäne gemacht werden. Diese Konfiguration kann einfach bereitgestellt und verwaltet werden.

Die optimale Konfiguration besteht also aus einer gemischten hierarchischen Anordnung der nternen und externen DNS-Namensräume. Die interne Domäne ist hierbei der externen

Namensraum *biotech.de* und der interne *intern.biotech.de* heißen. Mit der Differenzierung zwischen internen und externen Namensräumen wird sichergestellt, dass FQDNs immer eindeutig sind. Selbstverständlich können Sie unter *intern.biotech.de* auch noch weitere untergeordnete Domänen einrichten, wie zum Beispiel *berlin.intern.biotech.de*. Beachten Sie, dass für diese Konfiguration die für das Internet freigegebenen Server innerhalb Ihrer Domäne, aber außerhalb Ihrer Firewall stehen müssen.

Falls Sie die interne Domäne nicht als untergeordnete Domäne der externen Domäne konfigurieren, können Sie eine eigenständige Domäne verwenden. Es besteht dann kein Zusammenhang zwischen internen und externen Domänennamen, was unter Umständen zu Missverständnissen innerhalb der Benutzer führen kann. Es gibt keinen Bezug zwischen Ressourcen innerhalb und außerhalb Ihres Firmennetzwerks. Des Weiteren müssen Sie gleich zwei FQDNs über Ihren ISP bei der Internetnamensstelle registrieren lassen.

Die dritte Möglichkeit, denselben Domänennamen für den internen und externen Namensraum zu verwenden, verursacht aufgrund nicht eindeutiger DNS-Namen Probleme bei der Namensauflösung. Es kann sein, dass ein Host im internen Namensraum denselben Namen wie ein Host im externen Namensraum (Internet) besitzt. Obwohl Microsoft diese Vorgehensweise offiziell nicht empfiehlt, können Sie sie verwenden.

Wenden Sie einen der folgenden Schritte an:

- Sie können die Zonendaten vom externen DNS-Server auf den internen DNS-Server kopieren, wenn Ihre Clients Abfragen an externe Server (wie Webserver) durch eine Firewall weiterleiten.
- Falls die Clients keine DNS-Abfragen durch die Firewall leiten dürfen, können Sie die öffentlichen DNS-Zonendaten und alle öffentlichen Server auf einen Server in Ihrer Organisation kopieren.
- Verwalten Sie eine Liste der öffentlichen Server, die Ihrer Organisation gehören, in der Proxy-Autokonfigurationsdatei, die sich auf jedem DNS-Client befindet. Dies hört sich kompliziert an, kann jedoch mit dem Microsoft ISA-Server einfach durchgeführt werden.

> Wählen Sie einen internen Namensraum, und konfigurieren Sie diesen so, dass er dem externen Namensraum untergeordnet ist.

Entscheiden Sie, ob Sie einen internen DNS-Root benötigen

Die Entscheidung über einen DNS-Namensraum sollte eine der ersten sein, die Sie bei der Einführung von Active Directory treffen. Die erste Entscheidung ist natürlich die, überhaupt Microsoft-Produkte einzusetzen. Aber das ist natürlich auch ein wenig Firmenphilosophie.

Wenn Sie über ein umfangreiches und stark verteiltes Netzwerk und einen komplexen DNS-Namensraum verfügen, empfiehlt sich die Trennung des internen vom öffentlichen Namensraum. Dies klingt sofort logisch; Sie müssen allerdings, um dies zu gestalten, mit Aufwendungen für Server und Firewalltechnologie rechnen. Durch einen internen DNS-Namensraum

optimieren Sie die Verwaltung, da Sie nun die gesamte interne Infrastruktur so behandeln können, als ob der gesamte Namensraum innerhalb des Netzwerks bestehen würde.

ei einem internen DNS-Stamm wird eine private DNS-Stammzone auf einem oder mehreren DNS-Servern im internen Netzwerk gehostet. Der DNS-Server, der die private Stammzone hostet, wird als autorisierender Server für alle Namen im internen DNS-Namensraum etrachtet. Sie müssen allerdings dafür sorgen, dass Sie keine externen Namen im internen Namensraum verwenden, weil dies wegen der fehlenden Eindeutigkeit selbstverständlich zu ehlern führt.

Die Verwendung eines internen DNS-Stammes bietet Ihnen folgende Vorteile:

- Gute Skalierbarkeit
- Effiziente Namensauflösung für alle DNS-Clients, da keine Namensauflösungen über das Internet durchgeführt werden müssen.
- Keine Weiterleitungen. DNS-Server in einem internen DNS-Namensraum werden mit Stammhinweisen so konfiguriert, dass sie auf die internen DNS-Stammserver zeigen.

ACHTUNG

Wenn Sie allerdings Computer einrichten, die keinen Proxy unterstützen, oder wenn Sie ausschließlich Computer haben, die nur LATs (Local Address Table) unterstützen, können Sie keinen internen Stamm für den DNS-Namensraum verwenden!

In diesem Fall müssen Sie mindestens einen internen DNS-Server für das Weiterleiten von Anfragen an das Internet vorsehen. Für diese Aufgabe reicht auch ein Cache-only-DNS-Server aus.

st eine Namensauflösung für mehrere Topleveldomänen notwendig?

Wollen Sie für Windows Server 2003 Active Directory einen DNS-Namensraum zur Verfügung tellen, müssen Sie sicherstellen, dass die interne Namensauflösung korrekt funktioniert.

Wenn Sie Domänen oder DNS-Namensräume konsolidieren müssen oder wollen, müssen Sie die DNS-Namensauflösung als Erstes »stehen haben«. Hierzu können Sie eine der folgenden Vorgehensweisen wählen:

- Bei einem internen DNS-Stamm fügen Sie Delegierungen für jede DNS-Zone der obersten Ebene zur internen DNS-Stammzone hinzu.
- Die DNS-Server, die die Zone der höchsten Hierarchie-Ebene des ersten Namensraums hosten, müssen so konfiguriert werden, dass sie Abfragen an die Server der höchsten Hierarchie-Ebene des zweiten Namensraums weiterleiten. Gleiches gilt ebenfalls für den umgekehrten Fall. Hierfür können Sie auch eine bedingte Weiterleitung verwenden.

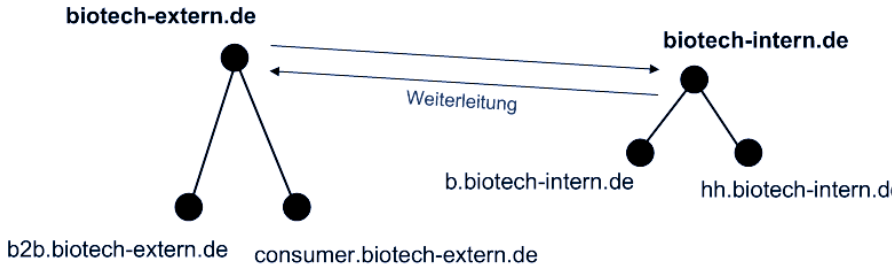


Abbildung 2.8: *Hosten zweier getrennter Namensräume für intern und extern. Hier ein Beispiel anhand der fiktiven Firma biotech.*

- Richten Sie jeweils in DNS-Servern mit den Zonendateien der obersten Hierarchie-Ebene des Namensraums eine sekundäre Zone ein, die eine Kopie des anderen Namensraums darstellt. Somit ist sichergestellt, dass alle DNS-Server in den beiden Namensräumen dieselben Informationen in den Zonendateien hosten. Diese Lösung verursacht allerdings eine hohe Replikationslast zwischen den DNS-Servern. Die DNS-Server selbst benötigen ebenfalls eine höhere Speicherkapazität.

Um die Datenverteilung zwischen den separaten Namensräumen zu erleichtern, können Sie Stubzonen verwenden. Beachten Sie jedoch, dass Stubzonen weniger effizient arbeiten als eine bedingte Weiterleitung. Stubzonen sind nur bei Windows Server 2003-Produkten möglich.

Windows Server 2003 DNS und eine bestehende DNS-Struktur

Microsoft Windows Server 2003 DNS ist mit den relevanten Internetstandards kompatibel und kann unter einigen Voraussetzungen auch mit anderen DNS-Implementierungen zusammenarbeiten. Je nachdem, welche Funktionen benötigt werden, können diese DNS-Implementierungen eingesetzt werden. Weitere Informationen finden Sie in *Kapitel 2.1.3*.

Erstellen Sie interne und externe Namensräume?

Sie entscheiden sich für einen internen und einen externen DNS-Namensraum. Um das Optimum dieser Konstellation zu gewährleisten, wird die interne Domäne der externen Domäne untergeordnet. Sie haben sich für diese Wahl entschieden, da sie Ihnen folgende Vorteile bringt:

- Es ist immer sichergestellt, dass interne Domänennamen eindeutig sind.
- Es muss lediglich der externe Name registriert werden.
- Die Verwaltung ist einfach, da Sie die Verantwortlichkeiten für die interne und die externe Domäne verteilen können.

Selbstverständlich können Sie Ihre untergeordnete interne Domäne zur übergeordneten Domäne für andere machen. Die Verwaltung obliegt allein dem »Administrator« des internen Namensraums. Beachten Sie jedoch, dass Sie die Computer, die Sie für den Zugriff über das Internet freigeben möchten, in Ihrer Domäne außerhalb der Internetfirewall bereitstellen. Alle anderen Computer stellen Sie hingegen in Ihrer untergeordneten internen Domäne bereit.

Planen und Erstellen von Internetnamen

SCHRITT FÜR SCHRITT

Gründet sich heutzutage eine Firma neu oder fusionieren Firmen miteinander, muss nach einem neuen Firmennamen gesucht werden. Hierbei sollten Sie darauf achten, dass Ihre Kunden Ihren neuen Firmennamen am besten intuitiv im Internet finden sollen. Sie müssen nicht nur interne DNS-Namen passend kreieren, damit sich die Mitarbeiter mit Ihrer Firma dentifizieren können, sondern Sie müssen auch externe öffentliche Namen finden, die Ihre neue Firma beschreiben, die aber noch nicht von anderer Seite reserviert wurden. Sind Sie international tätig, sollte der Name neben *.de* mindestens in den Topleveldomänen *.net*, *.com* und *.org* und ihren bevorzugten Länderdomänen vorhanden sein.

Fazit: Gehen Sie wie folgt vor:

1. Durchsuchen Sie das Internet, und überprüfen Sie, ob Ihre Wunschnamen verfügbar sind.
2. Überprüfen Sie, ob Sie Ihren Wunschnamen in Deutschland und in den gewünschten Ländern verwenden dürfen.
3. Ggf. müssen Sie den Namen käuflich erwerben oder gerichtlich gegen sog. Domänengrabber (Sammler) vorgehen.
4. Wenn die Punkte 1 und 2 erfüllt sind, melden Sie Ihre Internetdomänen und Ihre Firma an.
5. Bauen Sie Ihre Namensräume auf, indem Sie interne Namensräume und den externen Namensraum verwenden (im Einzelfall kann auch eine andere Konstellation verwendet werden).

ine komfortable Suche nach freien Domänennamen ist zum Beispiel unter `www.whois.sc` oder unter `www.icann.com` (Internet Corporation for Assigned Names and Numbers) möglich.

NetBIOS-Namen und DNS-Namen

Eine Besonderheit von Microsoft-Netzwerken ist die NetBIOS-Namensunterstützung. Für die Namensauflösung von NetBIOS gilt, dass sie voreingestellt über einen Broadcast an alle Mitglieder des gleichen Netzwerksegments gesendet wird. Haben Sie mehrere Netzwerksegmente, müsste ein Router den Broadcast durchlassen, was zu einem erhöhten unsinnigen Netzwerkverkehr führen würde. Vielmehr platziert man WINS-Server oder WINS-Proxies in die Segmente, um eine Datenbank für die Namensauflösung zu schaffen, ähnlich wie bei DNS. Leider sind DNS und WINS nicht kompatibel zueinander. Microsoft DNS kann jedoch mit WINS zusammenarbeiten, sodass DNS WINS-Abfragen tätigen kann.

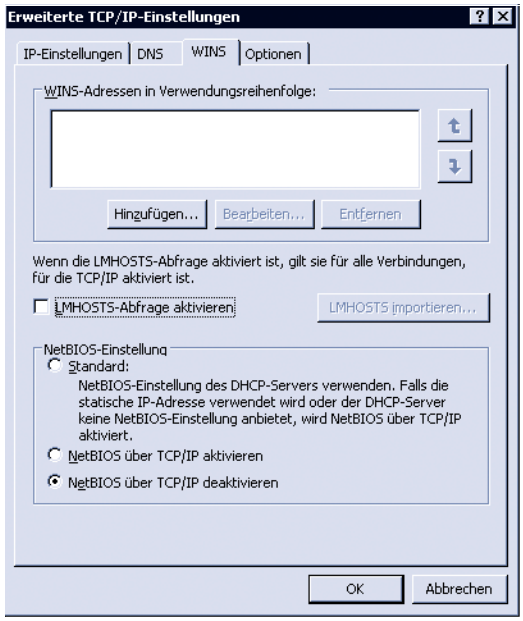


Abbildung 2.9: *NetBIOS muss bei jedem Computer über die Netzwerkkarteneigenschaften separat deaktiviert werden. Da ausschließlich mit DNS gearbeitet wird, können Sie die LMHOSTS-Abfrage ebenfalls deaktivieren. Beide Einstellungen sind standardmäßig aktiviert.*

Funktioniert die Namensauflösung über WINS (alternativ kann man auch eine Namensauflösung über LMHosts durchführen) nicht, können die Computer jeweils nur sich im jeweiligen Segment wiederfinden. Andere Computer in anderen Segmenten können nicht gefunden werden, da in der Regel der Router diesen Netzwerkverkehr blockiert.

Ohne WINS muss das Netzwerk auf Active Directory zurückgreifen, denn diesesbekommt seine Namen über DNS. Diese besondere Konstellation von WINS und DNS ist im Kursbuch über »*MCSE Windows Server 2003-Netzwerkinfrastruktur*« näher erläutert.

Müssen Sie eine gewisse Abwärtskompatibilität zu Windows NT sicherstellen, sind Sie auf WINS angewiesen. Windows Server 2003 DNS kann mit WINS zusammenarbeiten.

Wenn Sie Windows 2000 Server, Workstation oder Windows XP sowie Windows Server 2003-Produkte verwenden, können Sie ohne die NetBIOS-Unterstützung arbeiten. Entsprechend brauchen Sie sich keine Gedanken über den NetBIOS-Namen Ihrer Domäne zu machen. Andernfalls beachten Sie bitte, dass folgende Bedingungen gelten:

- Nicht zulässig sind Zahlen, Leerzeichen, Unicode-Zeichen sowie die Symbole: / \ < > [ ] : | + = ; , ? und *).
- Die maximale Länge des Namens beträgt 15 Zeichen.

Für Windows Server 2003 gilt RFC 2181, das heißt, dass DNS-Namen um beliebige Binärzeichenfolgen erweitert sind. Diese Binärzeichenfolgen müssen nicht als ASCII interpretiert werden. Des Weiteren gilt RFC 2044, das die Unterstützung der UTF-8-Zeichencodierung

UTF-8-Zeichensatz ermöglicht den Übergang von NetBIOS-Namen zu DNS-Namen. Standardmäßig wird die Multibyte-UTF-8-Namensüberprüfung verwendet.

HINWEIS

Andere Versionen von DNS unterstützen nur Zeichen, die nach RFC 1123 zugelassen sind. Verwenden Sie daher UTF-8-Zeichensätze nur dann, wenn ausschließlich Windows Server 2003 (und Windows 2000 Server) im Einsatz sind. Anders formuliert: Sie dürfen UTF-8 nicht im Internet verwenden.

Konsolidieren Sie DNS-Namensräume?

Das Zusammenführen von DNS-Namensräumen kommt insbesondere dann häufig vor, wenn zwei Organisationen mit unterschiedlichen Namensräumen fusionieren. Eine Umstrukturierung des gesamten Namensraums wäre unwirtschaftlich, daher greift man auf Methoden zurück, durch Weiterleitungen usw. den Namensraum zusammenwachsen zu lassen.

Entscheiden Sie auf der Grundlage von internen/externen Namensräumen, und entscheiden Sie, welche Domänen übergeordnete Instanzen für andere Domänen darstellen sollen.

Fallstudie: Vergabe von Namensräumen und FQDN

Situationsbeschreibung

Die Firma *Maschinenbau Müller GmbH* plant für ihre Businesspartner und Kunden einen eigenen Internetserver im Haus. Der Internetserver soll durch einen Router und eine Firewall einen direkten Zugang zum Internet haben und soll auch von dort erreicht werden. Man entscheidet sich, eine Internetdomäne mit einem aussagekräftigen Namen zu suchen. Die Firma Müller ist eine kleine mittelständische Firma mit 50 Angestellten, die insgesamt 60 Clientcomputer und 10 Server verwenden. Die Firma Müller ist ein Zulieferer eines großen Automobilkonzerns.

Abbildung 2.10 zeigt den Aufbau eines Netzwerks. Die Namen der Computer und die IP-Adressen des Perimeternetzwerks müssen noch bestimmt werden. Das Intranet (lokale Netzwerk) besitzt einen privaten Adressbereich (192.168.1.0/24), der bereits feststeht. Der interne Name der Windows Server 2003-Domäne steht bereits – aus historischen Gründen – mit *mueller.de* fest.

Das Perimeternetzwerk soll eine öffentliche IP-Netz-Adresse und der Internetserver eine feste öffentliche IP-Adresse bekommen. Man entscheidet sich auch, dass der gesuchte Internet Service Provider (ISP) dem Administrator der Müller GmbH so viel Arbeit wie möglich abnehmen soll.

Folgende Aufgaben sind durchzuführen:

- Festlegen des Namensraums bzw. der Namensräume
- Festlegen der FQDNs für den Internetserver
- Festlegen der IP-Adressen für den Internetserver
- Kommunikation mit dem ISP über die Namensverwaltung

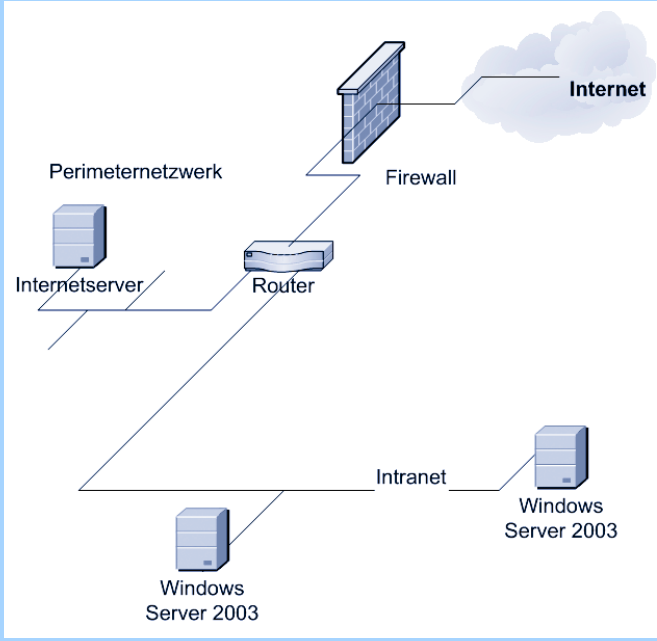


Abbildung 2.10: *Beispiel für eine Firma mit einem eigenen Internetserver*

Situationsanalyse

Vorgehensweise Subnetz

Nach einer Angebotsphase erhält der Provider den Zuschlag, der die geeignete Bandbreite per SDSL zur Verfügung stellt. Die Firma *Maschinenbau Müller GmbH* mietet das Nutzungsrecht für ein Subnetz mit den IP-Adressen 194.128.11.32/28 von ihrem Internet Service Provider (ISP). Der Administrator der Müller GmbH bestimmt, dass der Router die IP-Adresse 194.128.11.33 und der Internetserver die Adresse 194.128.11.34 erhält.

Vorgehensweise Namensraum

Da Umlaute im Domänennamen nicht möglich sind, entscheidet man sich für die Kurzform *mueller.de*. Nach einer Prüfung findet man heraus, dass die gewünschte Domäne in Deutschland vergeben ist. Man *mueller.de* zu nennen, da dieser Name noch verfügbar ist.

Somit liegt folgender Fall vor:

- Externer Namensraum: maschinen-mueller.de
- Interner Namensraum: mueller.de

Vorgehensweise DNS-Server/Zonen

Laut Vorgaben verwaltet der ISP den externen Namensraum von *maschinen-mueller.de*. Er trägt die gewünschten Daten (R-Records für den Internetserver) in die Zonendatei für seinen Kunden ein. Der DNS-Server des ISP kommuniziert im Namensraum des Internets mit anderen DNS-Servern. Die Müller GmbH besitzt keinen eigenen DNS-Server in ihrem öffentlichen Subnetz, da die Firma sich ja entschieden hat, den Aufwand möglichst gering zu halten.

Da Mitarbeiter jedoch direkten Zugriff auf den Internetserver benötigen, muss in irgendeiner Weise der interne DNS-Server Kenntnis von seiner IP-Adresse und seinem Namen erhalten. Dies kann auf unterschiedliche Weise geschehen:

- Bei einem internen DNS-Stamm *mueller.de* fügen Sie Delegierungen für die DNS-Zone *maschinen-mueller.de* zur internen DNS-Stammzone hinzu.
- Die DNS-Server, die die Zone der höchsten Hierarchie-Ebene des Namensraums *mueller.de* hosten, müssen so konfiguriert werden, dass sie Abfragen an die Server der höchsten Hierarchie-Ebene des zweiten Namensraums – hier beim Internetprovider – weiterleiten. Sie können auch eine bedingte Weiterleitung verwenden.

Eine nicht so schöne, aber funktionierende Lösung ist es auch, eine neue Zone in der höchsten Hierarchie-Ebene des Namensraums *mueller.de* zu erstellen, die nur einen A-Record (Name und IP-Adresse) des Internethosts enthält. Dieser Vorschlag ist bei einem so kleinen Netzwerk, wie es bei der Beispielfirma gegeben ist, akzeptabel.

Vorgehensweise FQDN

Nachdem ein externer Domänenname gefunden worden ist, können die Netzwerkcomputer im Perimeternetzwerk nach dem neuen Namensraum benannt werden.

Damit der Internetserver für die eigene Belegschaft auch freigegeben wird, muss eine DNS-Namensauflösung für die internen Computer funktionieren. In der Zonendatei der externen Domäne wird dem Internetserver ein interner und ein externer Name gegeben.

Üblicherweise wählt man als externen Namen (FQDN) *www.maschinen-mueller.de*. Beim internen Namen entscheidet man sich für den frei wählbaren Namen *asterix.mueller.de*. Der Name *asterix.mueller.de* ist der eigentliche FQDN, und *www.mueller.de* ist der zugehörige Aliasname. Der Aliasname soll hier der Internetname sein. Mitarbeiter können den Internetserver sowohl über den WWW-Namen als auch über den internen Namen ansprechen.

Vorgehensweise bei der DNS-Namensauflösung

Im DNS-Server beim Internetprovider wird der externe Internetname der Adresse 194.128.11.34/28 zugewiesen. Dieser Name wird auf jeden Internetserver auf der Welt repliziert. Jeder Internetbenutzer weltweit kann nun diesen Server finden, indem er in seinem Browser den Namen *www.maschinen-mueller.de* angibt.

Diskussion: Warum hat man sich für eine getrennte Namensauflösung entschieden?

Microsoft präferiert getrennte Namensräume, unterteilt in einen externen und einen internen Namensraum. Der interne Namensraum soll dem externen untergeordnet sein.

Da *mueller.de* als Domänenname für die bereits existierende Domäne vorgegeben ist, konnte diese Option nicht mehr gewählt werden. Ansonsten müssten Sie die Domäne umbenennen, was selbstverständlich mit viel Arbeit verbunden ist.

Bliebe noch die Option, die Internetdomäne und die Windows Server 2003-Domäne gleich zu benennen. Diese Option würde auch funktionieren, Sie müssen jedoch darauf achten, dass es zu keinen Überschneidungen mit den verwendeten Namen kommt. Beachten Sie, dass die Firma *Maschinenbau Müller GmbH* eine relativ kleine Firma ist.

Zusammenfassung

- Der Internetserver wurde für das Internet mit dem FQDN *www.maschinen-mueller.de* benannt.
- Für den internen Zugriff kann der Name *asterix.mueller.de* verwendet werden.
- Der interne Namensraum lautet *mueller.de*, während der externe Namensraum *maschinen-mueller.de* ist. Beide Namensräume sind voneinander getrennt.

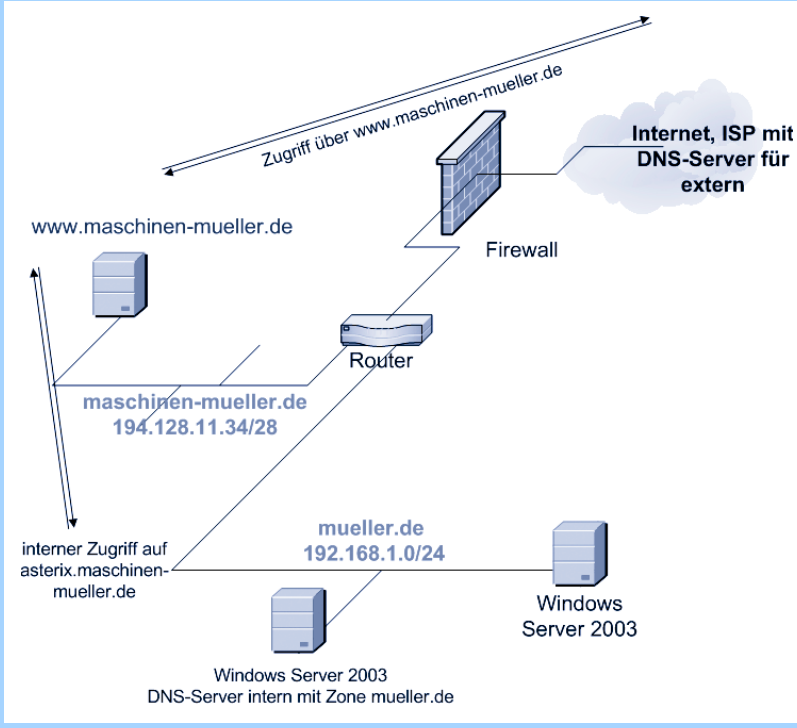


Abbildung 2.11: *Eine mögliche Lösung für eine externe- und interne Namensauflösung*

Fallstudie: Fusion zweier Namensräume

Situationsbeschreibung

Dieses Beispiel stammt aus Microsoft-Quellen und soll Sie gezielt auf die Prüfung vorbereiten: Die Firma *Contoso Corporation* fusioniert mit der Firma *Acquired Corporation*. Beide Firmen besaßen schon vor der Fusion einen eigenen Internetauftritt.

Vor der Fusion verwendete jedes Unternehmen interne Domänen, die jeweils untergeordnete Domänen der externen Domänen waren. Die *Contoso Corporation* benutzte für ihre DNS-Serververwaltung einen privaten Stamm. Die Firma *Acquired Corporation* leitete Abfragen an das Internet weiter, anstatt einen privaten Stamm zu verwenden. Es wurden auch keine Ausschlusslisten oder PAC-Dateien verwendet.

Aufgabe

Die Namensräume sollen zusammengeführt werden.

Situationsanalyse

Lösung

Der externe Namensraum des neuen, fusionierten Unternehmens enthält die Zonen *contoso.com* und *acquired.com*. Jede Zone im externen Namensraum enthält die DNS-Ressourceneinträge, die die Unternehmen im Internet bereitstellen möchten. Der interne Namensraum enthält entsprechend die internen Zonen *corp.contoso.com* und *corp.acquired.com*.

Beide Firmenteile entscheiden sich, eine unterschiedliche Methode zum Auflösen von Namen in ihren jeweiligen Namensräumen einzusetzen. Der Acquire-Teil soll weiterhin Anfragen direkt über das Internet weiterleiten. Der Contoso-Unternehmensteil verwendet den Namen *contoso.com* extern und entsprechend *corp.contoso.com* intern. Die internen Root-Server hosten die Stammzone (Rootzone) sowie die interne Zone *corp.contoso.com*.

Damit nun jeder DNS-Client innerhalb der fusionierten Organisation den gewünschten DNS-Namen auflösen kann, enthält die private Stammzone *corp.acquired.com* eine Delegation zu der Toplevelzone der fusionierten Organisation des internen Namensraums.

Wie in *Abbildung 2.12* zu erkennen ist, verwenden Clients der *corp.contoso.com* einen Proxyserver. Dieser wird für seine Namensauflösung den externen DNS-Server mit den beiden externen Zonen für *contoso.com* und *acquired.com* verwenden. Die Stammserver enthalten eine Delegierung zu der obersten Ebene des DNS-Namensraums der Unternehmenseinheit *Acquired*. Mit dieser Delegierung sind sie in der Lage, interne Namen von *Acquired* direkt und rekursiv zu beantworten, indem sie einen DNS-Server von *corp.acquired.com* abfragen.

Wie man ebenfalls aus *Abbildung 2.12* erkennt, fragen die internen DNS-Clients den internen DNS-Server, wenn sie Zugriff auf einen internen Computer benötigen. Enthält der angefragte DNS-Server nicht die gewünschten Daten, kann er durch eine rekursive Abfrage an andere interne DNS-Server den gewünschten internen Namen auflösen. Externe Namen können nicht aufgelöst werden, was für die Sicherheit im Netz spricht.

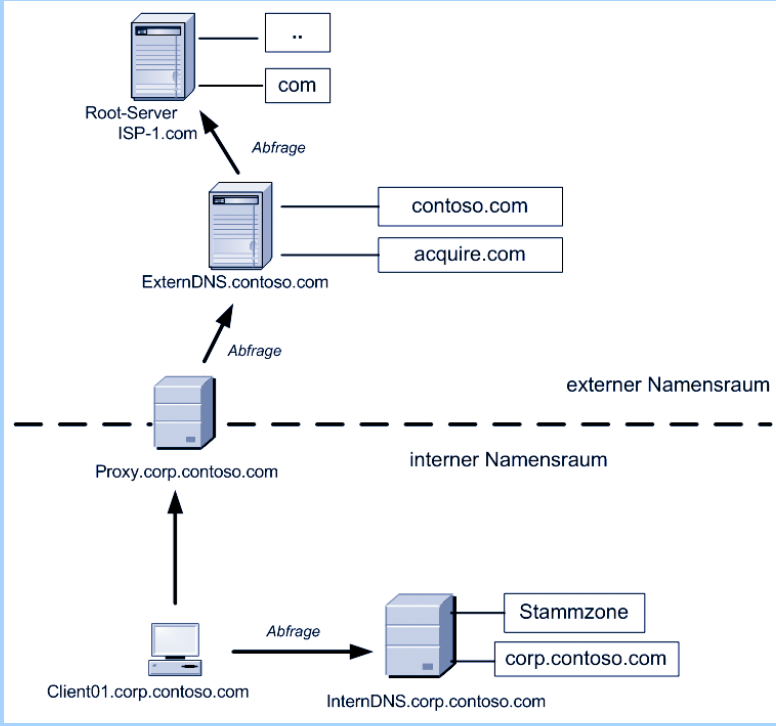


Abbildung 2.12: *Namensauflösung für den Unternehmensteil Contoso: Zugriff eines Clients auf die externe Domäne bzw. auf das Internet*

Wenn Clients einen Webzugriff oder einen Zugriff auf externe Computer der Firma Contoso durchführen müssen, verwenden Sie aus o.g. Sicherheitsgründen einen Proxyserver (zum Beispiel den Microsoft ISA Server oder einen Linux Squid Server). Dieser sendet eine ganz normale interaktive Anfrage an seinen bevorzugten DNS-Server (*ExternDNS.contoso.com*).

Für Computer aus dem Internet gilt, dass sie alle externen Namen von *Contoso* und *Acquired*, aber keine internen Namen (was zur Sicherheit des Netzwerks beiträgt) abfragen können.

Falls Clients von *Contoso* einen Zugriff auf Computer in dem Unternehmensteil *Acquire* benötigen, muss eine zusätzliche Verbindung zu dem internen DNS-Server von *Acquire* bestehen. Dies geschieht durch eine bedingte Weiterleitung. Sie erleichtert den Administratoren von *Acquire* die Verwaltungsarbeit. Wichtig für das folgende Modell ist, dass der interne DNS-Server von *Acquire* keine Stammzone besitzt. Er kann daher sonstige Abfragen direkt in das Internet bzw. zu externen Stammservern weiterleiten.

Achtung

Jeder DNS-Client kann nur einen bevorzugten DNS-Server bedienen. Nur wenn dieser ausfällt, kann ein weiterer DNS-Server abgefragt werden

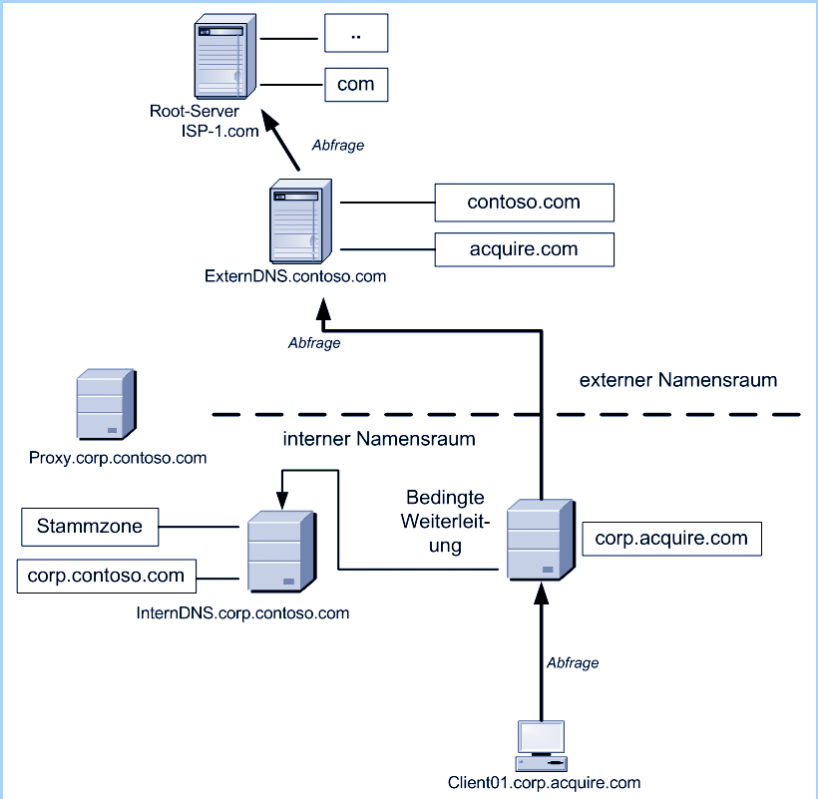


Abbildung 2.13: *Namensauflösung für Clients aus dem Acquire-Unternehmensteil.*

2.2.3 Design von DNS-Servern und Zonen

Nachdem Namensräume festgelegt worden sind, kann mit dem Design von DNS-Servern und Zonen begonnen werden. Wenn Sie Ihre DNS-Server planen, müssen Sie folgende Schritte beachten:

. Prüfen Sie, welche Hardware hierfür bereitsteht.

. Bestimmen Sie, wie viele DNS-Server Sie benötigen und an welchen Standorten sie stehen sollen.

Hardwarevoraussetzungen für DNS-Server

Laut Empfehlung von Microsoft sollte folgende Hardware (oder ähnlich leistungsfähige) für inen DNS-Server vorgesehen werden:

- Computer mit zwei Prozessoren mit 400-MHz-Pentium II-CPUs
- 256 MB RAM für jeden Prozessor

Es liegt auf der Hand, dass die Leistung mit stärkeren Prozessoren, Festplatten und mehr Hauptspeicher vergrößert wird. Jeder Ressourceneintrag benötigt ca. 100 Bytes RAM.

Anzahl DNS-Server

Um Ihren Verwaltungsaufwand zu verringern und eine Ausfallsicherheit sicherzustellen, sollten Sie mindestens zwei autorisierende DNS-Server für jede Zone festlegen. Zusätzliche Server für eine Zone können Sie einrichten, wenn Sie diese mit sekundären Zonen oder Active Directory-integrierten Zonen konfigurieren. Als Messlatte für die Leistungsfähigkeit eines DNS-Servers können Sie die dynamischen Aktualisierungen pro Sekunde heranziehen. Beispielsweise kann schon ein PIII-basierender Computer auf mehr als 10.000 Abfragen pro Sekunde reagieren.

Wenn Sie Zonen delegieren, fügen Sie zusätzliche DNS-Server zum Verarbeiten der delegierten Zonen hinzu. Beachten Sie jedoch, dass Sie keine Zonen delegieren müssen, wenn Sie über mehrere Zonen verfügen. Da ein Windows Server 2003 theoretisch 200.000 Zonen (mit 6 Ressourceneinträgen) hosten kann, können auch mehrere Zonen auf einem DNS-Server gehostet werden.

> Wenn Sie Zonen in Active Directory integrieren wollen, muss sich der DNS-Server auf einem Domänencontroller befinden!

Wägen Sie bitte immer den Replikationsverkehr bei Zonenübertragungen gegen den Datenverkehr bei iterativen/rekursiven Abfragen ab, auch wenn es sich positiv auswirkt, dass der DNS-Dienst eine inkrementelle Zonenübertragung unterstützt. In Verbindung mit DHCP, wo sich u.U. Leases oft verändern, kann dieses Leistungsmerkmal nicht nur die Replikation beschleunigen, sondern auch die Netzauslastung senken helfen.

Entscheiden Sie auch nach den Vorgaben Ihrer Netzwerktopologie. Wenn Sie über ein geroutetes LAN mit hoher Netzbandbreite verfügen, sind weniger DNS-Server notwendig, als wenn Sie viele eigenständige Segmente haben. Da geroutete LANs heutzutage Standard sind, kann somit die Topologie fast vernachlässigt werden. Um die Ausfallsicherheit wichtiger Netzteile zu gewährleisten, kommen Sie jedoch nicht umhin, DNS-Server in die jeweiligen (wichtigen) Segmente zu stellen.

Wenn Sie einen umfangreichen Namensraum mit vielen Clients verwalten, kommen Sie auf eine primäre und relativ viele sekundäre Zonen. Dies wird u.U. zu Überlastungen am primären DNS-Masternamenserver führen. Sie können dieses Problem folgendermaßen lösen:

- Verwenden Sie einige der sekundären Server als Masterserver für die Zone.
- Verringern Sie das Aktualisierungsintervall zu den sekundären Servern, wenn sich selten etwas an den Namen ändert.
- Erstellen Sie Cache-only-Server.

Standort des DNS-Servers

Da Sie immer auf eine maximale Verfügbarkeit Ihrer DNS-Server achten müssen, müssen Sie in sog. Einzelpunktversagen ausschließen. Daher sollten Sie zur Verbesserung der Fehleroleranz und Leistung mindestens zwei DNS-Server für jede Zone als autorisierende Server inrichten. Dabei platzieren Sie DNS-Server in verschiedene Subnetze, wenn Sie nur über ein okales Netzwerk verfügen. Falls Ihr Netz aus einem WAN und einem LAN besteht, platzieen Sie die DNS-Server, die für jede Zone autorisierend sind, in verschiedene Netze.

Wenn Sie ganz sichergehen wollen, dass die Namensauflösung nicht ausfällt, sollten Sie in jedem Subnetz mindestens einen DNS-Server einrichten. Die DNS-Clients sind dann nicht mehr auf die Funktionsfähigkeit von Routern angewiesen, vorausgesetzt, diese routen die DNS-Fragen weiter zu einem DNS-Server in einem anderen Netzwerksegment.

Wenn Sie ein Einzelpunktversagen in Ihrem Netzwerk entdecken, dann müssen Sie zunächst eststellen, ob der Fehler nur das DNS oder die gesamten Netzwerkdienste betrifft. Beachten ie, dass die Active Directory-Dienste einen funktionierenden Namenserver benötigen. Clients reifen auf DNS zurück, um Domänencontroller ausfindig zu machen! Der Exchange Server funktioniert zwar auch ohne einen Namensdienst, doch er kann u.U. keine E-Mails versenden.

TIPP

Es empfiehlt sich, in jedem Active Directory-Standort (Site) mindestens einen DNS-Server zu platzieren. Der Standort kann sich auch über mehrere Subnetze erstrecken.

Um die Ausfallsicherheit von Internetservern zu erhöhen, empfiehlt Microsoft den Einsatz on Offsite-DNS-Servern. Auch hier können Sie sich für primäre und sekundäre Offsite-DNS-Server entscheiden. Bedenken Sie jedoch den administrativen Aufwand, um diese Server gegenüber Hackerangriffe sicher zu machen. Seltsamerweise werden Offsite-Server uch dann von Microsoft empfohlen, wenn keine Internetpräsenz vorliegt.

2.2.4 Design von DNS-Zonen

Windows Server 2003-DNS-Zonentypen erfüllen jeweils einen bestimmten Zweck. Steht Ihr Namensraum und die Anzahl der DNS-Server fest, müssen Sie die Rolle der DNS-Server festlegen.

Sie haben folgende Auswahl:

- Primäre Zonen
- Sekundäre Zonen
- Stubzonen
- Reverse-Lookupzonen

rimäre Zonen, Reverse-Lookupzonen und Stubzonen können Sie in das Active Directory ntegrieren. Sie benötigen hierfür jedoch immer einen Domänencontroller mit einem DNS-Server. Sekundäre Zonen können Sie dagegen nicht in das Active Directory integrieren.

Fazit: Entscheiden Sie ebenfalls nach

- Ausfallsicherheit
- Lastenausgleich
- Netzlast, verursacht durch Replikation

Weitere Informationen zu den Zonen finden Sie in den vorangegangenen Kapiteln und im Werk »*MCSE Windows Server 2003-Netzwerkinfrastruktur*«.

2.2.5 Konfigurieren und Verwalten der DNS-Clients

Bei der Installation von Windows 2000/XP Professional-, Windows 2000 Server- und Windows Server 2003-basierenden Computern wird standardmäßig immer der DNS-Clientdienst installiert. Er wird beim Booten des Betriebssystems gestartet. Zudem muss in den Netzwerkeinstellungen der Netzwerkkarte die IP-Adresse von einem oder mehreren DNS-Servern eingegeben werden.

Beachten Sie, dass es immer nur einen einzigen bevorzugten DNS-Server gibt. Das gilt auch dann, wenn Sie mehrere DNS-Server eintragen. Der alternative DNS-Server wird nur dann vom DNS-Client abgefragt, wenn der primäre DNS-Server nicht verfügbar ist. Wählen Sie für den primären DNS-Server einen Server im lokalen Subnetz aus oder einen, der gut zu erreichen ist.

Per Default wird die DNS-Suffixsuchliste auf Grundlage des primären DNS-Suffixes des Clients und anhand von verbindungsspezifischen DNS-Suffixen aufgefüllt. Diese DNS-Suffixsuchliste können Sie mithilfe des DNS-Managers oder einer Gruppenrichtlinie ändern. Schränken Sie die Größe der Suffixsuchliste ein, um den Netzwerkverkehr zu minimieren.

Der Windows Server 2003 enthält einen verbesserten Satz von Gruppenrichtlinien, mit denen die Verwaltung von DNS-Clients vereinfacht wird.

2.2.6 Sichern der DNS-Infrastruktur

Als das Domain Name System (DNS) entworfen wurde, dachte man noch nicht an die Risiken, die mittlerweile im Internet vorkommen. Der Schutz vor Angriffen wurde nicht richtig bedacht. Die Risiken im Internet vollständig aufzuführen, würde den Umfang des Buchs sprengen. Deshalb sind hier nur einige wichtige Sicherheitsrisikenaufgeführt.

- Denial-of-Service-(DoS-)Angriff (Angriff auf den Dienst durch Überlastung)
- Footprinting (Auslesen von Informationen, die auf Typ, Aufgabe usw. schließen lassen)
- Datenmodifizierung (als Folge von Footprinting) bzw. IP-Spoofing
- Umleitung (um Anwendern z.B. falsche Internetseiten zu präsentieren)

Entwickeln einer Sicherheitsrichtlinie

ypischerweise besitzt (bei Microsoft) die Standardinstallation eine geringe Sicherheit. Das at einerseits den Vorteil, dass der Server immer gleich erfolgreich läuft, andererseits aber bie- et er ab der ersten Stunde potenziellen Angreifern die Möglichkeit, Ihren Server zu hacken.

ei der Installation werden bei Computergeräten, die mehrere Netzwerkkarten besitzen, tandardmäßig alle IP-Adressen verwendet. Die Rekursion ist ebenfalls aktiviert. Unter uhilfenahme der Rekursion können Angreifer durch DoS-Attacken den Server lahm legen. Des Weiteren findet man Hinweise auf das Stammverzeichnis. Durch das Bearbeiten der Stammserverliste werden die internen DNS-Server daran gehindert, private Informationen ber das Internet zu senden. Bedenken Sie auch, dass DNS-Server, die auch gleichzeitig Domänencontroller sind, eine DACL (Discretionary Access Control List) führen. Sie konfi- urieren die DACL über das Active Directory-Objekt *MicrosoftDNS* oder über die DNS-Managementkonsole, wobei letztere Methode empfohlen wird.

abelle 2.6 gibt Ihnen einen Überblick über die gefährdeten Bereiche und die empfohlenen Maßnahmen.

Gefährdete Bereiche	Maßnahme
Namensraum	Trennen Sie die interne von der externen Namensauflösung. Ein Mittel kann der Entwurf eines externen Namensraums sein.
Server	Modifizieren Sie die Standardeinstellungen für den DNS-Serverdienst in den Eigenschaften des Serverobjekts.
Zone	Modifizieren Sie die Standardeinstellungen für die Zonen in den Eigenschaften der jeweiligen Zone. Hier kann zum Beispiel auf sichere dynamische Updates zurückgegriffen werden.
Ressourceneintrag	Verwenden Sie DNS-Sicherheitsfunktionen von Active Directory-integrierten Zonen auf einem Domänencontroller.
DNS-Client	Steuern Sie die IP-Adressen der DNS-Clients.

abelle 2.6: *Sichern von DNS*

ei der Absicherung des DNS-Server spricht Microsoft von drei Sicherheitsstufen: Niedrig, Mittel und Hoch.

TIPP

Sicherheitsrichtlinien sind ein wichtiges Prüfungsthema.

DNS-Sicherheitsrichtlinie niedriger Sicherheitsstufe

Die niedrigste Stufe entspricht, wie bereits erwähnt, oft der Einstellung, die Sie nach der Installation vorfinden. Sie haben also keine nennenswerten Sicherheitsvorkehrungen getroffen. Daher sollten Sie diese Konfiguration nur in solchen Netzwerkumgebungen verwenden, die Sie als vertrauenswürdig erachten.

- Der Zugriff auf DNS-Server ist nicht beschränkt. Alle, einschließlich Clients und andere DNS-Server, können vom Internet aus auf den DNS-Server zugreifen.
- Alle DNS-Server im Netzwerk führen für jeden anfragenden Client eine DNS-Auflösung aus. Es gibt keine Beschränkung auf vertrauenswürdige Clients.
- Alle Server lassen Zonenübertragungen an beliebige Server zu.
- Der DNS hört alle auf einem Computergerät möglichen IP-Adressen.
- Die Funktion zur *Vermeidung von Zwischenspeicherbeschädigung* ist auf allen DNS-Servern deaktiviert.
- Die Weiterleitung und dynamische Aktualisierung ist für alle DNS-Zonen möglich.
- Beachten Sie auch, dass das Computergerät über keinerlei Firewall verfügt. Daher ist der DNS-Port 53 sowohl für UDP (User Datagram Protocol) als auch für TCP offen.

DNS-Sicherheitsrichtlinie mittlerer Sicherheitsstufe

Microsoft definiert die mittlere Sicherheitsstufe für Server, die ohne eine Active Directory-Integration laufen, aber folgende Merkmale aufweisen:

- Der Zugriff auf die DNS-Server ist teilweise beschränkt. Auf die DNS-Server Ihrer Organisation darf vom Internet aus – von bestimmten DNS-Servern – zugegriffen werden.
- Damit die Namensauflösung versuchen kann, alle gewünschten Namen aufzulösen, sind alle DNS-Server für die Verwendung von Weiterleitungen konfiguriert.
- DNS-Server übertragen Zonen nur an vertrauenswürdige DNS-Server. Diese Server sind die eingetragenen Namenserver.
- DNS-Server werden für das Abhören von bestimmten IP-Adressen konfiguriert. Eine dynamische Aktualisierung der IP-Adressen ist nicht zulässig.
- Der Einsatz einer Firewall schützt das interne Netzwerk vor unerlaubten Zugriffen von außen.
- Der Zugriff auf das Internet erfolgt über einen Proxyserver. Der interne E-Mail-Server erhält bzw. sendet über ein SMTP/POP3-Gateway Mails in das Internet.

DNS-Sicherheitsrichtlinie hoher Sicherheitsstufe

Microsoft definiert die hohe Sicherheit so, dass zu den Standardeinstellungen die Sicherheits-
unktionen für Active Directory-integrierte Zonen verwendet werden. Die mittlere Sicherheits-
stufe wird insofern verschärft, als keine Kommunikation mit dem Internet mehr möglich ist.
olgende Merkmale werden dieser Sicherheitsstufe zugeschrieben:

- Es gibt keine Kommunikation der DNS-Server mit dem Internet. Daraus folgt, dass es auch keinerlei Zonenübertragungen und Abfragen in das Internet gibt.
- Sie verwenden einen internen autarken DNS-Stamm.
- Die autorisierenden DNS-Server sind alle interne DNS-Server.
- Die Funktion zur Vermeidung von Zwischenspeicherbeschädigung ist auf allen DNS-Servern aktiviert.
- Dadurch, dass sich der DNS-Server auf einem Domänencontroller befindet, werden nur Active Directory-integrierte Zonen verwendet. So kann der Zugriff über die DACL gesteuert werden. Daraus resultiert, dass nur Berechtigungen für die Zone in Form von Erstellen, Löschen oder Ändern definiert werden können.
- Die sichere dynamische Aktualisierung ist aktiviert.

TIPP

Sichern Sie Ihren Server ab, bevor Sie ihn ins Netzwerk stellen. Dies ist insbesondere im Internet wichtig.

2.2.7 Arbeitsweise von DNS mit Active Directory

Der folgende Teil beschreibt Besonderheiten, die beim Gebrauch und bei der Integration in Active Directory in Erscheinung treten.

Verwendung von DNS, um Domänencontroller zu finden

SCHRITT FÜR SCHRITT

Damit sich ein Computer an einer Active Directory-Domäne anmelden kann, muss er einen Domänencomputer finden. Das könnte er zwar mit Hilfe eines Broadcasts tun, doch diese Methode funktioniert über geroutete Netzwerke nicht und verursacht außerdem noch viel Netzwerkverkehr. Je mehr Netzwerkverkehr auftritt, desto länger sind auch die Antwortzeiten des gesuchten Servers.

Microsoft hat aus Fehlern der Vergangenheit gelernt und die Domänencontrollerdienstinformationen in DNS integriert. Clients benötigen in den Netzwerkeigenschaften bzw. in den Eigenschaften der Netzwerkkarte die IP-Adresse des bevorzugten DNS-Servers.

Abbildung 2.14 verdeutlicht den Anmeldevorgang über den Anmeldedienst (Net Logon Ser-
ice) eines Mitglieds einer Domäne.

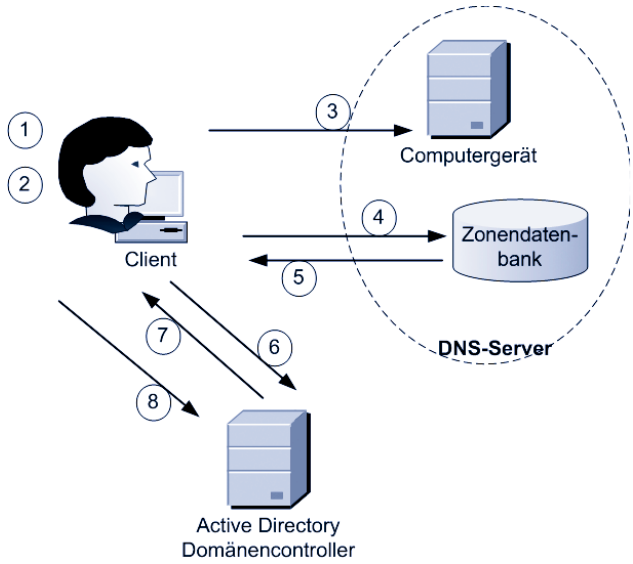


Abbildung 2.14: *So finden Clients den Domänencontroller.*

1 Ein Benutzer meldet sich interaktiv an einem Clientcomputer an, der Mitglied der Active Directory-Domäne ist. Der Anmeldedienst auf dem Clientcomputer initiiert eine Domänensuche und startet die *DsGetDcName API* (Application Programming Interface).

2 Der Anmeldedienst sammelt Informationen über den Client und den benötigten Dienst, um diese Informationen in die DNS-Abfrage zu integrieren. Hierbei sammelt die *DsGetDcName API* Informationen über den Standort, den Domänennamen und den Computernamen. Entsprechend lauten die *DsGetDcName*-API-Parameter *SiteName*, *DomainName* und *ComputerName*. Des Weiteren wird festgelegt, dass der Domänencontroller ein LDAP-Server der Domäne ist, wo sich auch der Client befindet. Auch die Informationen, dass der Domänencontroller ein KDC (Key Distribution Center) oder ein globaler Katalogserver ist, werden spezifiziert.

3 Der Anmeldedienst sendet eine DNS-Abfrage (DNS query) zum DNS-Server. Diese enthält die in Schritt 2 gesammelten Informationen.

4 Der DNS-Server fragt die Zonendatenbank nach SRV-Ressourceneinträgen ab, die zu der gesendeten Abfrage passen.

5 Der DNS-Server sendet eine Liste von IP-Adressen mit Domänencontrollern mit allen Informationen über die ursprüngliche Abfrage.

6 Der Anmeldedienst des Clients sendet ein spezielles Datagramm, eine LDAP-UDP-Meldung, zu einem oder mehreren Domänencontrollern, um festzustellen, ob die gewünschten Dienste verfügbar sind.

7 Jeder verfügbare Domänencontroller antwortet auf das Datagramm, um dem Client anzuzeigen, dass er ein potenzieller Anmeldeserver ist. Die zuerst erhaltene Verfügbar-

8 Der Clientcomputer wählt denjenigen Domänencontroller aus, der zuerst antwortet und den gesuchten Kriterien für die Dienste entspricht.

HINWEIS

Ein Clientcomputer benötigt folgende SRV-Ressourceneinträge:

- `_gc`
- `_kerberos`
- `_kpasswd`
- `_ldap`

Vorteile einer Active Directory-Integration

Wenn Sie Active Directory verwenden, empfiehlt Ihnen Microsoft die Integration von DNS-Zonen.

alls Sie sich für *Active Directory-integrierte Zonen* entscheiden, nutzen Sie folgende Vorteile:

- Erhöhung der Fehlertoleranz, weil jede Active Directory-integrierte Zone innerhalb der Gesamtstruktur repliziert werden kann. Die Replikation erfolgt über die Active Directory-Mechanismen und nicht über Einstellungen in der Zone.
- Zonen können mit der sicheren dynamischen Aktualisierung geschützt werden.
- Der Netzwerkverkehr verringert sich, da nur die veränderten oder neuen Informationen repliziert werden.

Einen kleinen Nachteil hat diese Vorgehensweise jedoch: Sie benötigen einen Domänen-ontroller mit einem DNS-Server.

Replikation von DNS-Zonen

Wenn Sie sich gegen eine Integration in Active Directory entscheiden, müssen Sie Folgendes beachten:

- Die DNS-Replikation beruht auf dem Prinzip des Einzelmastermodells. Fällt ein primärer DNS-Server mit seiner primären Zone aus, kann dies ein Einzelpunktversagen für die gesamte Zone bedeuten.
- Überwachen Sie Ihre primären DNS-Server, und stellen Sie immer den laufenden Betrieb sicher.

ie können Active Directory-integrierte Zonen und dateibasierte Zonen miteinander kombi-ieren. Für einen DNS-Server, der beispielsweise für Ihre private Stammzone autorisierend ist, können Sie auch ein anderes Betriebssystem als Windows Server 2003 oder Windows 2000 erver verwenden. Das trifft für BIND-Server genauso zu wie für Windows NT 4.0 Server. Diese Servertypen können nur dateibasierte Zonen hosten. Diese Zonen können Sie »anbin-den«, indem Sie sie an einen beliebigen Active-Directory-Domänencontroller mit DNS-Server delegieren.

Falls Sie Active Directory-integrierte Zonen in einer Windows Server 2003-Domäne verwenden, müssen Sie einen Active Directory-integrierten Zonenreplikationsbereich mithilfe der Managementkonsole auswählen. Beachten Sie weiterhin, dass die Auswahl eines großen Replikationsbereichs auch einen erhöhten Netzwerkverkehr zur Folge hat. Sollten Sie sich entscheiden, die Zonendaten an alle DNS-Server in der Gesamtstruktur zu replizieren, kann das eine sehr hohe Netzlast erzeugen. Sie sollten daher immer bestrebt sein, den Replikationsverkehr zu minimieren, indem Sie den Bereich so klein wie möglich, aber so groß wie notwendig gestalten. Die folgenden Replikationsoptionen für Windows Server 2003-basierte Domänencontroller helfen Ihnen dabei.

Replikationsoption	Beschreibung
Alle DNS-Server in der Active Directory-Gesamtstruktur	Die Zonendateien werden an alle DNS-Server (Domänencontroller) repliziert. Sie haben den breitesten Replikationsbereich ausgewählt und erzeugen den größten Replikationsverkehr. Sie können diese Option nur dann auswählen, wenn alle DNS-Server Windows Server 2003 ausführen und eine Active Directory-integrierte Kopie der Zone hosten.
Alle DNS-Server in einer angegebenen Active Directory-Domäne	Die Zonendateien werden nur an diejenigen Domänencontroller in der angegebenen Domäne repliziert. Diese Option ist die Standardeinstellung für die Active Directory-integrierte DNS-Zonenreplikation. Sie schränken mit dieser Option den Zonenreplikationsverkehr ein. Beachten Sie auch hier, dass Zonendaten nicht an DNS-Server repliziert werden, die sich auf Windows 2000-basierten Domänencontrollern befinden.
Alle Domänencontroller in der Active Directory-Domäne	Die Zonendaten werden an alle Domänencontroller in der angegebenen Active Directory-Domäne repliziert. Dies geschieht unabhängig davon, ob ein DNS-Server auf dem jeweiligen Domänencontroller in der Domäne ausgeführt wird. Diese Möglichkeit steht Ihnen zur Verfügung, wenn Sie Windows 2000-basierte Domänencontroller haben.
Alle Domänencontroller, die im Replikationsbereich einer Anwendungsverzeichnispartition angegeben wurden	Die Zonendaten werden an alle Domänencontroller repliziert, die im Replikationsbereich der Anwendungsverzeichnispartition angegeben wurden. Diese Option kann den Replikationsverkehr effektiv minimieren. Sie benötigen hierfür Windows Server 2003-basierte Domänencontroller mit dem DNS-Serverdienst.

Tabelle 2.7: *Replikationsoptionen für Windows Server 2003-basierte DNS-Server, die als Domänencontroller eingerichtet sind*

Die Aktualisierung (Update) der DNS-Namen

Betriebssysteme wie die folgenden aktualisieren ihren DNS-Namen (Fully Qualified Domain Name, FQDN) automatisch beim Booten, Anmelden usw. an der Domäne in der Zonendatenbank des DNS-Servers:

- Windows Server 2003-Familie
- Windows 2000 Server-Familie
- Windows 2000 und XP Professional

Für diese Computer besteht der primäre FQDN aus dem sog. primären DNS-Suffix und dem Computernamen. Wenn Sie den Aktualisierungsvorgang näher betrachten, können Sie feststellen, dass dieser immer dann auftritt, wenn:

- Der Computer neu startet.
- Eine Adresse hinzugefügt, entfernt oder modifiziert wird.
- Ein IP-Adress-Lease sich ändert oder erneuert wird.
- Manuell `ipconfig /registerdns` in die Eingabeaufforderung eingegeben wird.
- Ein Mitgliedsserver zum Domänencontroller heraufgestuft wird.

Durch ein dynamisches Update ist eine manuelle Verwaltung von Zoneneinträgen, wie A-Records für die Clients nicht mehr notwendig. Dynamische Updates sind in RFC 2136 eschrieben und stellen eine wesentliche Erleichterung bei der Verwaltung dar. Der DNS-Serverdienst bietet die Möglichkeit, dynamische Updates auf Zonenbasis auf jedem Server zu ktivieren oder zu deaktivieren. Der DNS-Client versucht jedoch nicht standardmäßig dynamische Updates zu Zonen der obersten Ebene durchzuführen. Für diesen Fall müssen Sie entweder die Registrierung ändern oder die Richtlinieneinstellung »Domänenzonen der bersten Ebene aktualisieren« verwenden. Zusätzlich wird dieses Feature noch erweitert, wenn die Zone Active Directory-integriert ist. Mit Hilfe der ACL können Sie dann festlegen, welche Computer ein Update durchführen dürfen.

Beachten Sie, dass bei der Verwendung von DHCP nicht der DNS-, sondern der DHCP-Clientservice ein dynamisches Update triggert. Der dynamische Updateprozess von DHCP-Clients nterscheidet sich von dem hier beschriebenen dynamischen Update über DNS.

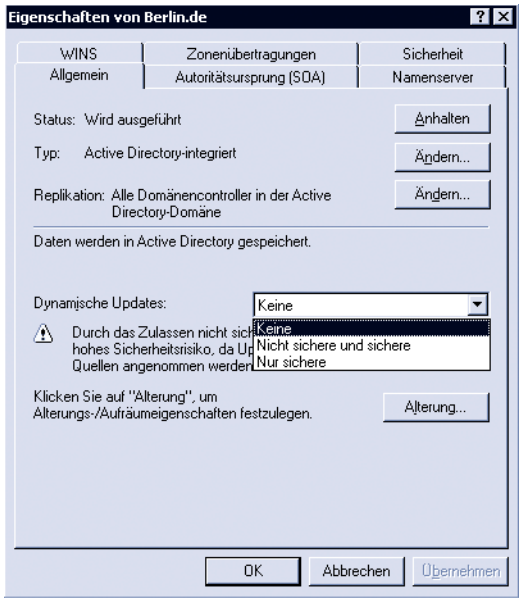


Abbildung 2.15: *Dynamische Updates können in den Eigenschaften der etreffenden Zonen eingestellt werden.*

Prinzipiell gibt es drei verschiedene Arten, ein Update durchzuführen (siehe auch *Abbildung 2.15*):

- Dynamisches Update für alle Computer. In der Einstellung KEINE können Updates von nicht vertrauenswürdigen Quellen angenommen werden.
- Nicht sicheres und sicheres dynamisches Update
- Zulassen von nur sicheren Updates für Domänenmitglieder

Integration von DHCP in DNS

Ein DHCP-Server, der auf einem Windows Server 2003 läuft, kann dynamische Updates im DNS-Namensraum für jeden Client durchführen, der diese Updates unterstützt. Eine dynamische Aktualisierung findet immer dann statt, wenn eine Änderung der DHCP-zugewiesenen Adresse stattfindet. Die Aktualisierung betrifft nicht nur A-Records, sondern auch PTR-Records. Für diesen Vorgang wird eine zusätzliche DHCP-Option benötigt, die Client-FQDN-Option (Option 81). Diese Option ermöglicht es dem Client, den zugehörigen FQDN und Anweisungen zur Verarbeitung von DNS-dynamischen Aktualisierungen dem DHCP-Server zur Verfügung zu stellen.

Eine praktische neue Seite beim DHCP-Server ist die Unterstützung von Computergeräten mit Windows-Betriebssystemen, die keine dynamische Aktualisierung unterstützen. Diese sog. Legacy-Clients, die nicht in der Lage sind, die Option 81 an den DHCP-Server zu senden, können so konfiguriert werden, dass sie ähnlich wie die modernen Clients eine dynamische Aktualisierung bekommen. Somit können auch hier A- und PTR-Records der Clients verändert bzw. verworfen werden, wenn der Clientlease sich verändert und der Lease gelöscht wird.

Der DHCP-Clientservice ist wegen der Integration in dem DNS-Server auch dann notwendig, wenn der Computer nicht als DHCP-Client konfiguriert wird. Stellen Sie den DHCP-Clientservice ab, können keine dynamischen Updates mehr stattfinden. Auch der Befehl `ipconfig /registerdns` funktioniert dann nicht mehr.

Mehr Infos zum DHCP-Dienst finden Sie in dieser Reihe im MCSE-Kursbuch »*Windows Server 2003-Netzwerkinfrastruktur*« zur Prüfung 70-291.

Sichere dynamische Updates

Sichere dynamische Updates sind nur für Active Directory-integrierte Zonen verfügbar. Nachdem Sie diesen Zonentyp erstellt haben, können Sie je nach Bedarf die ACL (Access Control List) editieren, um den Zugriff auf diese Zone zu steuern. Voreingestellt behandeln Windows Server 2003-Computer ein sicheres dynamisches Update wie folgt:

- Einstellung *Nicht sichere und sichere*: Windows Server 2003-DNS-Clients versuchen zuerst eine nicht sichere Aktualisierung durchzuführen. Falls dies fehlschlägt versuchen sie es mit einer sicheren. Bei der Aktualisierung sind die Clients in der Lage, eine bestehende Konfiguration zu überschreiben (Standard).

- Einstellung *Nur sichere*: Wie die Bezeichnung schon treffend beschreibt, dürfen nur sichere Updates von vertrauenswürdigen Clients durchgeführt werden. Wer als vertrauenswürdig gilt, können Sie über die Access Control Lists steuern.

Nachdem eine Zone in eine Active Directory-integrierte Zone umgewandelt wurde, sind nur sichere dynamische Updates zulässig.

HINWEIS

Wenn Sie eine Standard-Zone verwenden, also keine Active Directory-integrierte Zone, ist kein dynamisches Update voreingestellt.

2.2.8 Integration von Windows Server System-Applikationen

Der Microsoft DNS-Server bietet Ihnen eine Vielzahl von Integrationsmöglichkeiten. Auf einige, wie die Integration in Zonen auf BIND-Servern ist bereits eingegangen worden. Andere, wie die Zusammenarbeit mit WINS und DHCP, werden Sie in den folgenden Abschnitten kennen lernen. Besonderes Augenmerk ist hierbei auf die Neuerungen von Windows Server 2003 gelegt worden.

Besonderheiten der Integration von DNS in DHCP

Wenn Sie für die dynamische Verteilung von IP-Adressen in Ihrem Netzwerk DHCP (Dynamic Host Configuration Protocol) einsetzen, müssen Sie dieses so konfigurieren, dass alle DHCP-Clients neben einer gültigen IP-Adresse auch Informationen über den DNS-Server rhalten. Weiterhin sollten die DHCP-Clients auch eine dynmische IP-Adressenaktualisierung urchführen können. Dieses Feature ist im RFC 2136 (»Dynamic Updates in the Domain Name System«) beschrieben.

Als DHCP-Server dürfen Sie Windows 2000 Server- und Windows Server 2003-Produkte erwenden. Sie können über die dynamische Aktualisierung A- und PTR-Ressourceneinträge erstellen bzw. aktualisieren. Zum Löschen der veralteten Einträge muss jedoch die Alterungsnd Aufräumfunktion aktiviert werden.

ei der dynamischen Aktualisierung wird die FQDN-Option 81 verwendet. Sie erst ermögcht, dass der DHCP-Client seinen FQDN (Fully Qualified Domain Name) bereitstellen ann. Des Weiteren wird auch beschrieben, wie dynamische Aktualisierungen vom DHCP-Server verarbeitet werden sollen. Der DHCP-Server ist in der Lage,

- sowohl DNS-A-Einträge für Forward-Lookupzonen als auch PTR-Einträge für Reverse-Lookupzonen zu aktualisieren (mit Option 81).
- DNS-A- und PTR-Einträge unabhängig von der Anforderung des Clients zu aktualisieren.

ehr vorteilhaft ist es auch, dass für Windows NT-Clients eine dynamische Aktualisierung möglich ist.

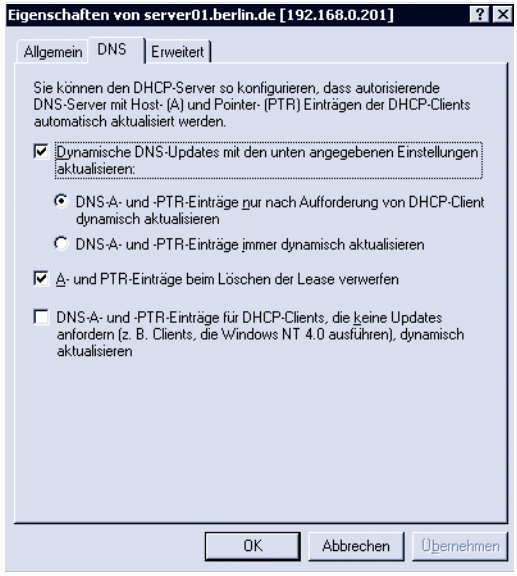


Abbildung 2.16: *Konfigurieren des DHCP-Servers im Snap-In DHCP*

Besonderheiten für die Integration von WINS in DNS

Das Microsoft *Windows Internet Name System* (WINS) stellt die dynamische Variante der NetBIOS-Namensauflösung dar. Sie kann anstelle einer LMHOSTS-Datei verwendet werden. Sie benötigen WINS nur dann, wenn Sie eine NetBIOS-Namensauflösung über mehrere Subnetze tätigen müssen.

Da es früher keine dynamische Aktualisierung bzw. Registrierung von Windows NT- oder Windows 98-Clients (oder von noch älteren Versionen) gab, konnte man einen WINS-Lookup verwenden, damit die A-Ressourceneinträge in der Zone erstellt und aktualisiert wurden. Über einen Reverse-Lookup konnten analog dazu PTR-Ressourceneinträge erstellt und aktualisiert werden.

WINS-Server sind in einem modernen Netzwerk, das aus Betriebssystemen der Windows 2000- und Windows Server 2003-Produktfamilie besteht, nicht notwendig. Ein Abschalten hat hier den Vorteil, dass die TCP- und UDP-Ports 137 geschlossen werden können.

2.3 Einrichten eines DNS-Servers

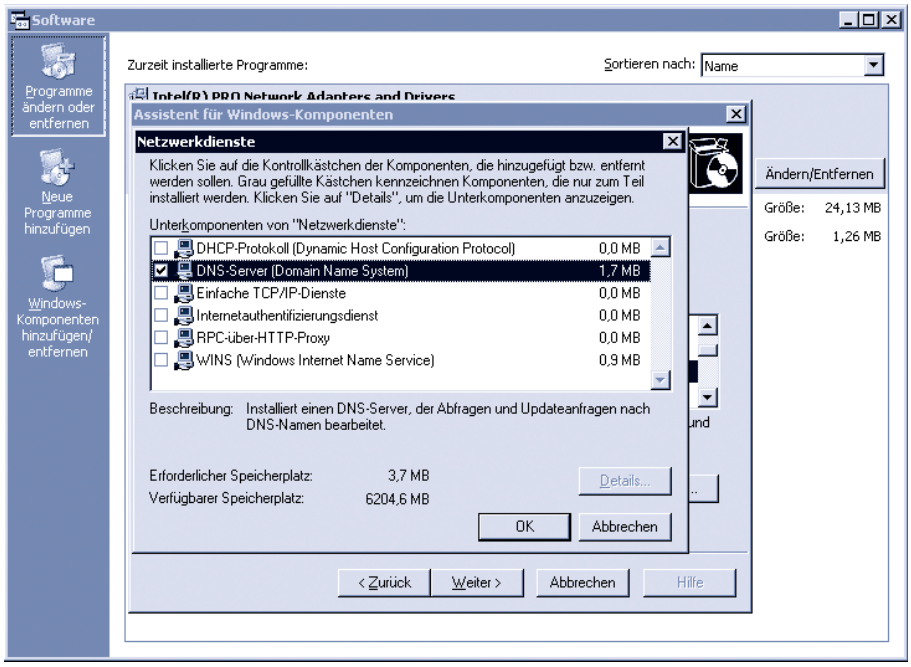
Das Einrichten eines DNS-Servers ist, wie bei vielen Microsoft-Diensten unproblematisch. Direkt nach der Installation kann er seine Arbeit aufnehmen. Zu beachten ist jedoch, dass anfangs auch alle sicherheitskritischen Einstellungen aktiviert sind.

evor Sie jedoch den DNS-Dienst installieren, überprüfen Sie die Netzwerkverbindung zu anderen Hosts. Dies können Sie mit dem Dienstprogramm *ping* in der EINGABEAUFFORDERUNG zu einigen ausgesuchten Computern durchführen. Somit gehen Sie sicher, dass alle Clients den DNS-Server über die IP-Adresse finden können. Weiterhin dürfen Sie einem DNS-Server keine dynamische IP-Adresse über DHCP vergeben, da er auch bei Ausfall des DHCP-Servers verfüg- ar sein muss. Entsprechend bekommt der DNS-Server eine statische IP-Adresse zugeteilt.

2.3.1 Installation

Mit einer der folgenden zwei Methoden können Sie einen DNS-Server installieren:

- Über die Systemsteuerung unter SOFTWARE und WINDOWS KOMPONENTEN HINZUFÜGEN. Anschließend können Sie mit dem Assistenten für die DNS-Serverkonfiguration Lookup- und/oder Reverse-Lookupzonen erstellen und konfigurieren.
- Während der Installation eines Domänencontrollers. Er wird nicht nur automatisch installiert, sondern auch für den Gebrauch von Active Directory korrekt konfiguriert. Dieser Vorgang erspart Ihnen Zeit und vermeidet zudem Fehler.



2.3.2 Werkzeuge zur Konfiguration

Neben der normalen Administration über die Managementkonsole (Snap-In *dnsmgmt.msc*) kann der DNS-Server auch über folgende Programme konfiguriert werden:

- Mit dem Kommandozeilenprogramm `DNSCmd.exe`
- Mit einem VB-Script oder anderen Scriptsprachen, die den WMI-(Windows Management Instrumentation)-Anbieter verwenden

Insbesondere mit dem Kommandozeilenprogramm `DNSCmd.exe` kann eine Konfiguration per Batchdatei schnell und einfach durchgeführt werden.

Das Kommandozeilenprogramm DNSCmd.exe

Das folgende Programm eignet sich für den späteren Gebrauch in Projekten sehr gut und wird Ihnen daher als zusätzliche Information kurz vorgestellt.

Das Kommandozeilenprogramm *DNSCmd* finden Sie in den Support-Tools von Microsoft, die sich neben dem Betriebssystem ebenfalls auf der Installations-CD befinden. Das Tool zeigt und ändert die Eigenschaften eines DNS-Servers. Dies betrifft Zonen genauso wie Ressourceneinträge (Records). *DNSCmd* erweitert das bereits von Windows NT bekannte Dienstprogramm *DNSStat.exe*.

Sie können das Programm wie folgt starten:

```
dnscmd <ServerName> Kommando [Kommando-Parameter]
```

Hier können Sie als Servernamen sowohl die IP-Adresse als auch den DNS-Namen des Hosts angeben.

Die folgenden Kommandos sind zulässig:

Kommando	Kurzbeschreibung
`/Info`	Anzeigen von Konfigurationseinstellungen, wie Domänenname oder DS-Container.
`/Config`	Anhand von insgesamt 47 Kommandoparametern können Server- und Zoneneinstellungen angepasst werden. Der Parameter `/Config` erlaubt eine Änderung der Werte in der Registrierung (Registry).
`/EnumZones`	Gibt eine Liste von Zonen heraus.
`/Statistics`	Fragt oder löscht die DNS-Serverstatistik mit dem entsprechenden Kommandoparameter.
`/ClearCache`	Löscht den DNS-Server-Cache.
`/WriteBackFiles`	Diese Operation aktualisiert solche Zonen, bei denen Änderungen im Arbeitspeicher noch nicht in den nicht flüchtigen Speicher (persistent storage) geschrieben wurden. Die Operation kann alle oder nur bestimmte Zonen überprüfen.

Tabelle 2.8: *Befehlssatz von* `DNSCmd.exe`

Kommando	Kurzbeschreibung
`/StartScavenging`	Dieser Parameter bestimmt, wann ein Server mit dem Aufräumen dieser Zone beginnen kann.
`/ResetListenAddresses`	Verändert die bestehende IP-Adresse unter Angabe einer neuen Adresse, auf die der DNS-Server hört.
`/ResetForwarders`	Stellt den DNS-Server so ein, dass er rekursive Anfragen zu einem bestimmten Forwarder sendet. Einstellungen, ob der DNS-Server iterative Anfragen tätigt oder nicht, sind ebenso möglich.
`/ZoneInfo`	Zeigt Zoneninformationen an.
`/ZoneAdd`	Fügt eine neue Zone auf dem DNS-Server hinzu. Sie können angeben, welcher Art (Active Directory-integriert etc.) die Zone sein soll.
`/ZoneDelete`	Löscht eine bestehende Zone auf dem DNS-Server oder in Active Directory.
`/ZonePause`	Pausiert die Zone: Alle Anfragen an die DNS-Zone werden ignoriert.
`/ZoneResume`	Startet die Zone, die vorher pausierte.
`/ZoneReload`	Der Befehl kopiert die Zoneninformationen von seiner Quelle (Zonendatei oder Verzeichnisdienst) in den Arbeitsspeicher.
`/ZoneWriteBack`	Ähnlich wie das Kommando `/WriteBackFiles`; mit der Ausnahme, dass hier nur eine spezifische Zone ausgewählt wird.
`/ZoneRefresh`	Bewirkt die Aktualisierung einer sekundären Zone.
`/ZoneUpdateFromDs`	Bewirkt eine Aktualisierung der Active Directory-integrierten Zone. Dieser Vorgang geschieht voreingestellt alle 5 Minuten mit der normalen Aktualisierung des Active Directory.
`/ZonePrint`	Zeigt alle Ressourceneinträge in der spezifizierten Zone an.
`/ZoneResetType`	Ändert den Zonentyp einer bestimmten angegebenen Zone nachträglich. Falls der DNS-Server sich auf einem Domänencontroller befindet, kann die Zone Active Directory-integriert werden.
`/ZoneResetSecondaries`	Gibt eine Liste von IP-Adressen an, auf die der Masterserver antwortet, sobald er einen Zonentransfer starten soll.
`/ZoneResetScavengeServers`	Betrifft den Aufräumvorgang: Ändert die IP-Adresse des oder derjenigen Server, die den Aufräumvorgang der bestimmten Zone durchführen dürfen.
`/ZoneResetMasters`	Verändert die IP-Adresse des Masterservers auf Servern, die sekundäre Zonen hosten. Der Wert für die IP-Adresse des Masterservers wird erstmalig beim Erstellen einer sekundären Zone in die Eigenschaften der Zone eingetragen.

Tabelle 2.8: *Befehlssatz von* `DNSCmd.exe` *(Forts.)*

Kommando	Kurzbeschreibung
`/ZoneExport`	Erstellt eine Textdatei mit den Inhalten der betreffenden Zone.
`/ZoneChangeDirectory-Partition`	Ändert die Verzeichnispartition, auf der sich die bestimmte Zone befindet: Mögliche Speicherorte sind die Domänen- oder Gesamtstruktur-Verzeichnispartitionen. Eine sog. Legacy-Partition für Prä-Windows Active Directory-Domänencontroller ist ebenfalls möglich.
`/EnumRecords`	Listet alle Ressourceneinträge einer bestimmten Zone auf.
`/RecordAdd`	Fügt einen Ressourceneintrag einer Zone hinzu. Alle Ressourceneintragstypen werden unterstützt (A-Record, MX-Record usw.).
`/RecordDelete`	Entfernt einen Ressourceneintrag.
`/NodeDelete`	Entfernt alle Ressourceneinträge auf einem Host (also Vorsicht!).
`/AgeAllRecords`	Diese Operation dient der Abwärtskompatibilität zu älteren DNS-Servern, bei denen ein Aufräumvorgang (Scavenging) nicht unterstützt wird. Der Eintrag fügt dem Ressourceneintrag einen Zeitstempel (time stamp) mit der aktuellen Zeit hinzu.
`/EnumDirectoryPartitions`	Listet alle Verzeichnispartitionen auf.
`/DirectoryPartitionInfo`	Zeigt Informationen über eine bestimmte Verzeichnispartition an.
`/CreateDirectoryPartition`	Erstellt eine Anwendungsverzeichnispartition von DNS. Beachten Sie, dass bei der Installation von DNS eine Anwendungsverzeichnispartition für den Dienst auf Domänen- und Gesamtstrukturebene erstellt wird. Mit der Operation `/CreateDirectoryPartition` können Sie noch weitere Verzeichnispartitionen hinzufügen.
`/DeleteDirectoryPartition`	Löscht eine Anwendungsverzeichnispartition.
`/EnlistDirectoryPartition`	Fügt den DNS-Server zu einem bestimmten Replikationsbereich, der für die Verzeichnispartition zuständig ist, hinzu. Der FQDN der Verzeichnispartition ist als Eingabe notwendig.
`/UnenlistDirectoryPartition`	Stellt die Umkehroperation zu `/EnlistDirectoryPartition` dar und entfernt den DNS-Server aus dem Replikationsbereich.
`/CreateBuiltinDirectory-Partitions`	Falls Sie irrtümlich die Standard-Anwendungsverzeichnispartitionen gelöscht haben, können Sie sie mit diesem Kommando wiederherstellen.

Tabelle 2.8: *Befehlssatz von* `DNSCmd.exe` *(Forts.)*

Das folgende Beispiel zeigt Ihnen die Verwendung dieses Dienstprogramms. Hierbei ist *Berlin.de* eine DNS-Zone:

```
dnscmd berlin.de /enumzones
```

Wenn Sie das Ergebnis in eine Textdatei exportiert haben wollen, müssen Sie folgenden Befehl in der Kommandozeileneingabe eingeben:

```
dnscmd berlin.de /enumzones > Textdatei.txt
```

Sie bekommen für die Zone *Berlin.de* folgende Ausgabe:

```
Enumerated zone list:
  Zone count = 4

  Zone name                    Type       Storage         Properties
  .                            Cache      File
  _msdcs.Berlin.de             Primary    AD-Forest       Secure
  0.168.192.in-addr.arpa       Primary    File            Rev
  Berlin.de                    Primary    AD-Legacy

Command completed successfully.
```

Listing 2.2: *Ausgabe der Zonen nach Installation eines Active Directory (Überprüfung der Installation)*

Wie Sie aus dem oben gezeigten Listing erkennen können, besitzt der DNS-Server folgende Zonen, wobei *Domänenname* der benutzerdefinierte Name der DNS-Domäne, bzw. der Active Directory-Domäne ist:

- _msdcs.*Domänenname*
- 0.168.192.in-addr.arpa
- *Domänenname*

2.3.3 Wichtige Verwaltungsarbeiten

Das Verwalten und Einrichten eines DNS-Servers geschieht in der Regel im Verwaltungsprogramm DNS bzw. im Snap-In `dnsmgmt.msc`.

HINWEIS

Dieses Teilkapitel setzt voraus, dass Sie sich mit Active Directory-Strukturen und insbesondere Domänencontrollerfunktionen, wie globale Katalogserver, Key Distribution Server usw., auskennen.

Hier wird lediglich auf die Besonderheiten in Verbindung mit Active Directory hingewiesen. ür mehr Informationen hinsichtlich des DNS-Servers sind das »*Windows Server 2000 Resource Kit*« und das MSCE-Kursbuch zur Prüfung 70-291 zu empfehlen.

Einrichten eines DNS-Stammservers

Nach der Installation ist der DNS-Server automatisch immer als Stammserver konfiguriert. Wenn Sie keinen Stammserver benötigen, müssen Sie die Stammzone löschen.

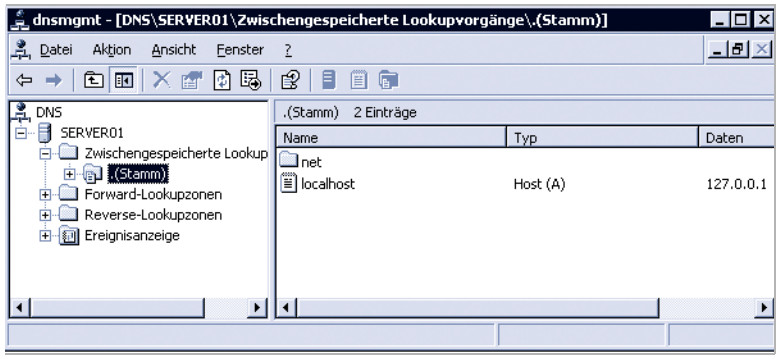


Abbildung 2.18: *Verwaltung des DNS-Servers über die Managementkonsole: Stammzonen beim Windows DNS-Server*

Überprüfen einer DNS-Server-Installation

Nach der Installation eines Active Directory können Sie überprüfen, ob der DNS-Server ordnungsgemäß läuft und konfiguriert ist. Falls Sie eine automatische Konfiguration durch den Assistenten zum Installieren von Active Directory vornehmen lassen, enthält der DNS-Server nicht nur die gewünschte Zone, sondern auch alle notwendigen SRV-Ressourceneinträge.

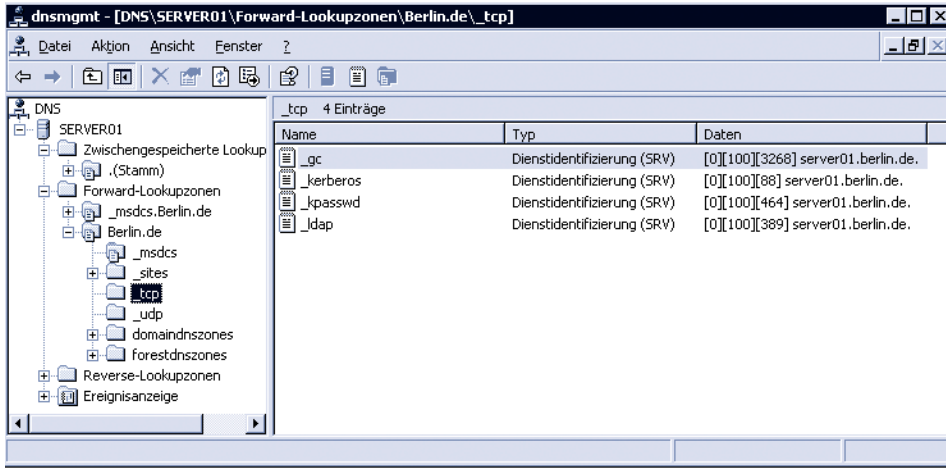


Abbildung 2.19: *Überprüfung der neu erstellten Zone (berlin.de stellt hier den internen Namensraum dar.)*

Überprüfung der SRV-Ressourceneintragsformate

Damit die Active Directory-Dienste ordnungsgemäß funktionieren können, muss der DNS-Server *Service Resource Records* (SRV-Records) unterstützen. SRV-Records erlauben es Clientomputern, den Domänencontroller zu lokalisieren, denn sie müssen sich auf diesem mit Ihrem Computerkonto authentifizieren. Mit den SRV-Records wird ein Server als Domänenontroller identifiziert. Daher enthält ein SRV-Record nicht nur den Computernamen, sondern auch den Namen des Dienstes und weitere dienstspezifische Angaben.

Mit einem SRV-Ressourceneintrag (SRV-Record) können Sie:

- einen Domänencontroller in einer Active Directory-Domäne oder -Gesamtstruktur identifizieren.
- einen Domänencontroller (Abkürzung *dc*) in seinem Standort identifizieren.
- einen Domänencontroller, der als *Globaler Katalog Server* (Abkürzung *gc*) definiert ist, identifizieren.
- einen Domänencontroller mit dem *Kerberos Key Distribution Center*-(KDC-)Service identifizieren.

Domänencontroller (gemeint sind hier nur Domänencontroller der Windows 2000 Server- nd Windows Server 2003-Familie) registrieren somit folgende SRV-Records im DNS-Dienst:

SRV-Recordtypen	Beschreibung
ldap._tcp. DnsDomainName	Ermöglicht es Computern, einen LDAP-Server in der Domäne zu finden. Alle Domänencontroller besitzen diesen Eintrag.
ldap._tcp. SiteName**._sites.dc._msdcs.**DnsDomainName	Ermöglicht es Computern, einen Domänencontroller in dem gleichen Standort (wie der Computer) zu finden. Alle Domänencontroller besitzen diesen Eintrag.
gc._tcp. DnsForestName	Ermöglicht es Computern, einen globalen Katalogserver zu finden. Beachten Sie, dass der Domänenname der Name der Stammdomäne (forest root domain) ist. Nur Domänencontroller, die als globale Katalogserver konfiguriert sind, bekommen diesen Eintrag.
gc._tcp. SiteName**._sites.**DnsForestName	Ermöglicht es Computern, einen globalen Katalogserver in dem gleichen Standort (Site) zu finden. Nur Domänencontroller, die als globale Katalogserver konfiguriert sind, bekommen diesen Eintrag.
_kerberos._tcp. DnsDomainName	Ermöglicht es Computern, einen KDC-Server in der gleichen Domäne zu finden. Da auf allen Domänencontrollern auch der Kerberos V5-Dienst läuft, besitzen sie ebenfalls diesen Eintrag.
_kerberos._tcp. SiteName**._sites.**DnsDomainName	Ermöglicht es Computern, einen KDC-Server in dem gleichen Standort zu finden. Alle Domänencontroller besitzen diesen Eintrag.

abelle 2.9: *Kurzbeschreibung der SRV-Records*

Ein SRV-Ressourceneintrag verwendet ein definiertes Format. Dieses lautet:

```
_service_.protocol.name TTL class SRV priority weight port target
```

Beispiel:

```
_gc._tcp 600 IN SRV 0 100 3268 server01.berlin.de
```

Listing 2.3: *Syntax und Anwendung des SRV-Recordformats.*

Feld (deutsche Übersetzung)	Beschreibung
_Service (Dienst)	Beschreibt den Namen des Dienstes (wie beispielsweise LDAP oder Kerberos), den der Server unterstützt.
_Protocol (Protokoll)	Beschreibt den Typ des Transportprotokolls (wie TCP oder UDP).
Name (Domäne)	Beschreibt den Domänennamen.
TTL (Gültigkeitsdauer)	Time to Live: Gibt in Sekunden an, wie lange der Wert ohne Überprüfung gültig ist.
Class	Beschreibt den Standardressourceneintragsklassenwert. Dieser beträgt immer »IN« für das Internet System.
Priority (Priorität)	Beschreibt die Priorität. Clients wenden sich immer an den Host mit der niedrigsten Priorität.
Weight (Gewichtung)	Beschreibt einen Lastverteilungsmechanismus, den Clients verwenden, wenn sie einen Zielhost suchen. Falls der Wert für das Gewicht für zwei Computer der gleiche ist, wählen Clients einen davon nach einem Zufallsprinzip aus. Ansonsten wird der SRV-Record mit dem höchsten Gewicht ausgewählt.
Port (Portnummer)	Gibt den Port (Anschluss) an, der für diesen Dienst vorgesehen ist. Liegt eine Firewall zwischen dem Client und dem Server, muss die Firewall diesen Port für den entsprechenden Dienst freigeben.
Target (Host, der diesen Dienst anbietet)	Beschreibt den FQDN des Computers, der den entsprechenden Dienst unterstützt.

Tabelle 2.10: *Beschreibung der Parameter eines SRV-Ressourceneintrags*

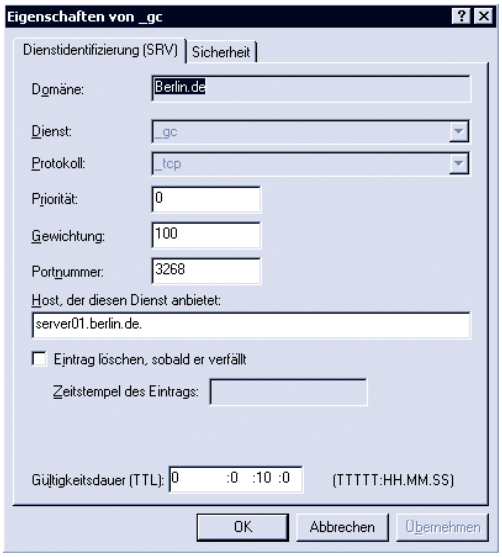


Abbildung 2.20: *Darstellung der Eigenschaften eines SRV-Records eines Domänencontrollers*

HINWEIS

Neben Active Directory-Domänencontrollern kann ein Netzwerk auch Computer enthalten, die nicht Windows-Server sind, aber als LDAP-Server konfiguriert sind. Diese Server bekommen in den entsprechenden Zonen die SRV-Records zur Dienstidentifizierung hinzugefügt.

Anwendungsverzeichnispartitionen

Anwendungsverzeichnispartitionen für Active Directory-integrierte DNS-Zonen werden zur eduzierung von Replikationsverkehr verwendet. Sie verringern ebenso die Menge der Daten, die in einem globalen Katalog gespeichert werden. Anwendungsverzeichnispartitionen sind ein Feature von Windows Server 2003. Wenn Sie eine Aktualisierung von Windows 2000-basierten Domänencontrollern vornehmen, verschieben Sie die Active Directory-interierten DNS-Daten auf allen DNS-Servern von der Domänenpartition zu der neu erstellten Anwendungsverzeichnispartition. Dieser Schritt ist vorgenommen, wenn Sie den Replikatinsbereich der DNS-Zonen verändern.

ie können DNS-Zonen, die Sie zu allen DNS-Servern in der Gesamtstruktur (Forest) replizieen wollen, in die gesamtstrukturweiten DNS-Anwendungsverzeichnispartitionen verschieben. Diese Anwendungsverzeichnispartitionen haben die Bezeichnung *ForestDnsZone*.

ACHTUNG

Stellen Sie bei einem Migrationsprojekt zu Windows Server 2003 vor der Verschiebung der DNS-Daten auf eine Anwendungsverzeichnispartition sicher, dass der *Domänennamenmaster* (Domain Naming Master) sich auf einem Windows Server 2003-Domänencontroller befindet.

Sollte die *_msdcs.forest_root_domain* als separate Zone nicht vorhanden sein, benötigen Sie keinen Verschiebevorgang, da die DNS-Daten bereits mit der Stammdomänenzone zu der domänenweiten Anwendungsverzeichnispartition *DomainDnsZones* verschoben worden sind. Diese speziellen Partitionen werden automatisch bei der Installation einer Gesamtstruktur in jeder Active Directory-integrierten DNS-Zone installiert. Falls das Einrichten der Anwendungsverzeichnispartition fehlschlägt, versucht der DNS-Dienst sie jedes Mal neu zu erstellen, sobald der Dienst neu gestartet wird.

Die folgenden Anwendungsverzeichnispartitionen werden voreingestellt installiert:

- *ForestDnsZones* für den Geltungsbereich Gesamtstruktur
- *DomainDnsZones* für den Geltungsbereich Domäne

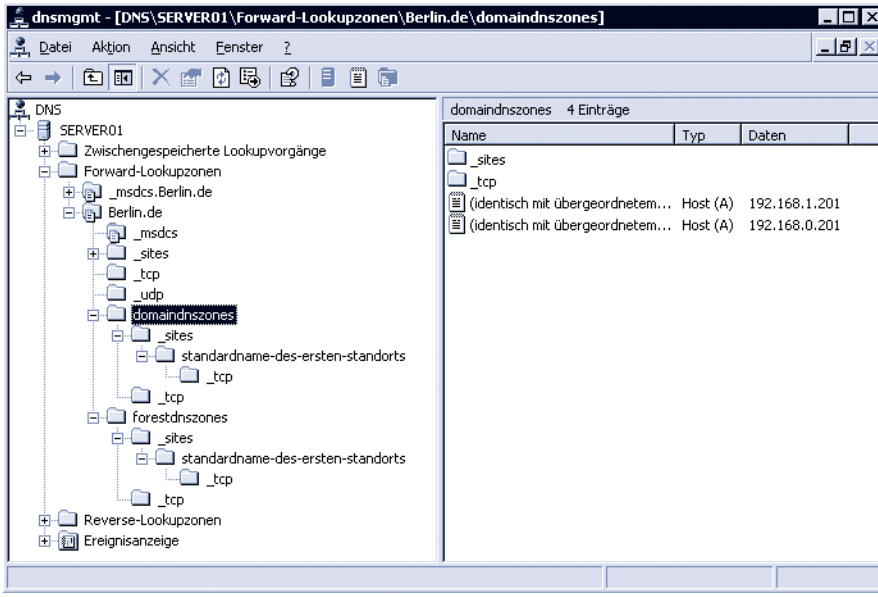


Abbildung 2.21: *Anwendungsverzeichnispartitionen bei einer Active Directory-integrierten DNS-Zone*

Die besondere Rolle der Zone _msdcs.ForestName

Dieser Abschnitt beschreibt die besondere Rolle der Zone *_msdcs.ForestName*, die immer benötigt wird, wenn ein Upgrade von Windows 2000 Server auf Windows Server 2003 erfolgt, aber auch immer installiert wird, wenn der Assistent für die Installation des Active Directory (`dcpromo.exe`) den DNS-Server konfiguriert.

In diesen Fällen wird automatisch eine Forward-Lookupzone erstellt, die das Präfix *_msdcs* enthält und den Namen der Gesamtstruktur (ForestName). Wenn, wie in den o.g. Beispielen beschrieben, als Name der Gesamtstruktur *berlin.de* gewählt wurde, heißt die entsprechende Zone dann *_msdcs.berlin.de*.

Die zweite erstellte Zone entspricht einer normalen, für die Domäne erstellten Zone, wie Sie es auch von Windows 2000 Server her kennen. Diese Zone stellt die Microsoft-Stammdomäne (Root Forest Domain) dar. Sie wird zwischen den DNS-Servern bzw. den Domänencontrollern der Domäne synchronisiert. Die Beschreibung dieser Zone können Sie in den vorangegangenen Abschnitten nachlesen.

Die *_msdcs.ForestName*-Zone ist in der gesamtstrukturweiten Anwendungsverzeichnispartition gespeichert.

Wenn Sie einen Windows 2000 Server- zu einem Windows Server 2003- Domänencontroller ktualisieren wollen, benötigen Sie keine Modifizierungen an der DNS-Zonenkonfiguration. Die *_msdcs.ForestName*-Zone wird auf einem der folgenden Wege gespeichert:

- Fall 1: Die *_msdcs.ForestName*-Zone ist eine Subdomäne der Active Directory-integrierten Stammdomänenzone. Die sekundären *_msdcs.ForestName*-Zonen sind in Ihren untergeordneten Domänen gespeichert, falls diese vorhanden sind.
- Fall 2: Die *_msdcs.ForestName*-Zone ist eine Subdomäne in Ihrer Active Directory-integrierten Stammdomänenzone.

Nachdem alle DNS-Server in der Stammdomäne mit dem Windows Server 2003-DNS-Server-Dienst laufen, konfigurieren Sie Ihre Gesamtstrukturzone so, dass sie in einer Active Directory-integrierten domänenweiten Anwendungsverzeichnispartition gespeichert ist. Alternativ können Sie auch eine Directory-integrierte gesamtstrukturweite Anwendungsverzeichnispartition einrichten, falls Sie diese benötigen.

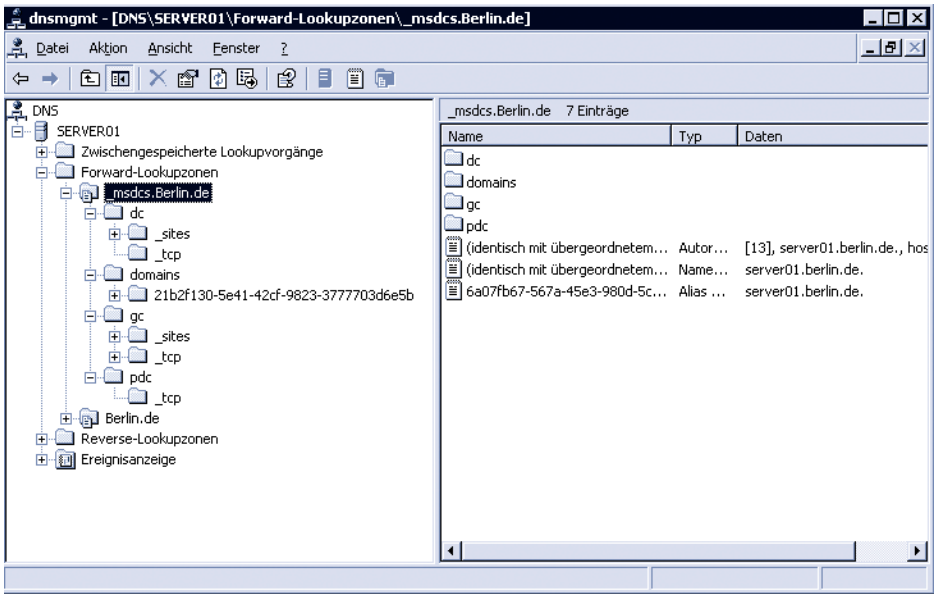


Abbildung 2.22: *Darstellung der _msdcs.ForestName-Zone*

Zusammenfassung

In der Lernzielkontrolle werden Sie neben Übungen zur Prüfung auch Fragen und die Antworten zu Prüfungsfragen finden.

Das *Kapitel 2* hat Ihnen den Zusammenhang zwischen DNS-Namensauflösung und Active Directory Services vermittelt. Hierbei wurde ein besonderer Schwerpunkt auf

- das Grundverständnis von DNS,
- die Funktion und
- die Integration in Active Directory

gelegt.

Berücksichtigen Sie folgende entscheidende Punkte im Hinblick auf eine Active Directory-Installation:

1. Bevor Sie eine Active Directory-Struktur planen, konzipieren Sie den DNS-Namensraum! Identifizieren Sie den Namen, den Sie oder Ihre Firma für die Verwendung im Internet hat registrieren lassen.
2. Falls Sie einen Internetauftritt haben oder planen, sollten Sie unterschiedliche Namensräume für interne und externe DNS-Namen verwenden. Wählen Sie am besten eine untergeordnete Domäne des externen Namens für Ihre Microsoft-Stammdomäne.
3. Verwenden Sie für Computer, die im Internet freigegeben sind, externe DNS-Namen und von ihnen verschiedene interne DNS-Namen. Verwenden Sie einen Webproxy.
4. Der DNS-Server muss die Fähigkeit haben, SRV-Einträge zu unterstützen. Wenn Sie das Microsoft DNS von Windows Server 2003 verwenden, bekommen Sie alle unterstützenden Features.
5. Windows Server 2003 DNS bietet Active Directory-integrierte Zonen mit einigen Vorteilen, die Sie in Betracht ziehen sollten.
6. Wenn Sie eine erhöhte Sicherheit und eine verbesserte Replikation planen, sind Active Directory-integrierte Zonen die bessere Wahl. Die Konsequenz hieraus ist, dass der Domänencontroller auch gleichzeitig DNS-Server wird.

Obwohl es auch funktioniert, für den Internetauftritt einen gleichen Domänennamen für die interne wie auch die externe Domäne zu wählen, bevorzugt Microsoft das Modell der übergeordneten externen Domäne im Internet zur untergeordneten internen Microsoft-Domäne. Beachten Sie dies bitte in der Prüfung.

2.4 Lernzielkontrolle

2.4.1 Wiederholungsfragen

Die folgenden Fragen helfen Ihnen bei dem Durcharbeiten des Kapitels. Die Reihenfolge der hemen ist bewusst gemischt, d.h., Sie müssen hier nicht chronologisch vorgehen.

Die Lernzielkontrolle gibt Ihnen die Möglichkeit, den theoretischen Stoff anzuwenden. Da das DNS nicht primär das Thema des Buches und der Prüfung ist, ist es hinsichtlich der allemeinen Wartung des DNS-Servers verkürzt worden.

Sie finden daher auch hier überwiegend Übungen, die sich auf Active Directory beziehen. Einige der fortgeschrittenen Übungen sind nur zu verstehen, wenn Sie die Funktionsweise des Active Directory kennen. Also, liebe Leserin, lieber Leser, wenn Sie schon fit sind, dann st der fortgeschrittene Teil das Richtige für Sie!

Alle anderen Leser bitte ich, erst einmal weiterzulesen und den fortgeschrittenen Teil später zu bearbeiten.

Die folgenden Fragen helfen Ihnen beim Durcharbeiten des Stoffs (die Antworten finden Sie in *Kapitel 2.4.5*):

1. Wie unterscheidet sich ein Namensraum von einer Microsoft-Domäne?
2. Warum ist die Planung des DNS-Namensraums so wichtig für Active Directory?
3. Wer entscheidet bei der Planung des Namensraums?
4. Welche besonderen Features hat ein Windows Server 2003-DNS-Server?
5. Können für Active Directory auch Nicht-Windows-DNS-Server verwendet werden?
6. Wie verhält es sich mit Windows NT- und Windows 98-Clients hinsichtlich einer dynamischen Aktualisierung?
7. Welche Replikationsmechanismen gibt es?

2.4.2 Allgemeine Computereinstellungen in den Übungen

Sie finden einige allgemeine Einstellungen in vielen Übungen vor. Alle Übungen sind so konipiert, dass Sie sie auch mit anderen Namen für den Computer, die Domäne, die Gesamtstruktur usw. durchführen können.

Auf eine Fixierung auf Beispielnamen ist bewusst verzichtet worden. Es ist bei vielen Übungen auch selbstverständlich, dass Sie ein administratives Konto verwenden müssen. Sollten Sie gar Privilegien als Organisations-Admin oder Schema-Admin benötigen, werden Sie daauf hingewiesen.

Eingabeaufforderung

Bei einigen Übungen werden Befehlszeilenprogramme in die Eingabeaufforderung eingegeben. Sie können diese wie folgt verwenden:

- Klicken Sie zum Öffnen der EINGABEAUFFORDERUNG auf START, klicken Sie auf PROGRAMME, dann auf ZUBEHÖR und anschließend auf das Feld EINGABEAUFFORDERUNG.
- Alternativ können Sie die EINGABEAUFFORDERUNG ausführen, wenn Sie auf START und dann auf AUSFÜHREN klicken. In das Eingabefeld geben Sie dann den Befehl `cmd` ein.

Verwendeter Domänencontroller und Domäne

In den Übungen wird ein Domänencontroller mit den folgenden Daten verwendet (die Informationen wurden mit dem Befehl `ipconfig /all` ausgelesen):

```
Windows-IP-Konfiguration

    Hostname  . . . . . . . . . . . . : Server01
    Primäres DNS-Suffix . . . . . . . : Berlin.de
    Knotentyp . . . . . . . . . . . . : Unbekannt
    IP-Routing aktiviert  . . . . . . : Nein
    WINS-Proxy aktiviert  . . . . . . : Nein
    DNS-Suffixsuchliste . . . . . . . : Berlin.de

Ethernet-Adapter Intel Pro 1000 MT Gigabit Ethernet Adapter - onboard:

    Verbindungsspezifisches DNS-Suffix:
    Beschreibung  : Intel(R) PRO/1000 MT Network Connection
    Physikalische Adresse . . . . . . : 00-07-E9-55-44-F8
    DHCP aktiviert  . . . . . . . . . : Nein
    IP-Adresse. . . . . . . . . . . . : 192.168.1.201
    Subnetzmaske  . . . . . . . . . . : 255.255.255.0
    Standardgateway . . . . . . . . . :

Ethernet-Adapter Intel Fast Ethernet LAN Controller - PCI slot 4:

    Verbindungsspezifisches DNS-Suffix:
    Beschreibung  . . : Intel(R) PRO/100B PCI Adapter (TX)
    Physikalische Adresse . . . . . . : 00-A0-C9-43-83-AD
    DHCP aktiviert  . . . . . . . . . : Nein
    IP-Adresse. . . . . . . . . . . . : 192.168.0.201
    Subnetzmaske  . . . . . . . . . . : 255.255.255.0
    Standardgateway . . . . . . . . . :
```

Listing 2.4: *Bildschirmausgabe von* `ipconfig /all` *eines Domänencontrollers mit dem Hostnamen* `Server01`

Windows Server 2003 Support Tools

Viele der nachfolgend gezeigten Übungen benötigen die Microsoft Windows Server Support ools. Sie finden diese Tools auf der Windows Server 2003-Installations-CD unter:

```
E:\SUPPORT\TOOLS
```

TIPP

Viele der in den Microsoft Support Tools und im Ressource Kit vorhandenen Dienstprogramme werden auch in der Prüfung abgefragt.

2.4.3 Übungen für Einsteiger

Die folgenden Übungen sind durchzuführen, wenn Sie lediglich Kenntnisse des laufenden Kapitels und/oder Grundkenntnisse in Active Directory besitzen.

Überprüfen der DNS-Konfiguration

iel: Nach der Installation des ersten Domänencontrollers soll die DNS-Server-Konfiguration überprüft werden.

Voraussetzungen

Sie benötigen die folgenden Vorkenntnisse:

- Kenntnisse über DNS-Server

ür diese Übung benötigen Sie Folgendes:

- Einen Windows Server 2003-basierten Domänencontroller

Vorgang: Sie installieren eine Active Directory-Domäne mit dem *Assistenten zum Installieren von Active Directory*. Sie lassen ihn alle Einstellungen für das Active Directory vornehmen.

Aufgaben

Überprüfen Sie folgende Sachverhalte:

1. Welche Zonen und Zonentypen werden erstellt?
2. Wie sieht die Replikation der DNS-Zonen aus?
3. Welche Rolle spielt der Anmeldedienst bei der Konfiguration der Domänencontroller?
4. Welche SRV-Record-Typen gibt es, und wie hängen diese mit einem Domänencontroller zusammen?

Die Antworten auf diese Fragen finden Sie in *Kapitel 2.4.6*.

Lösungshilfen

SCHRITT FÜR SCHRITT

1 Klicken Sie auf START, dann auf VERWALTUNG und anschließend auf DNS.

2 Klicken Sie in der DNS-Konsole auf FORWARD-LOOKUPZONEN, und doppelklicken Sie auf die Zone.

3 Identifizieren Sie die *_msdcs.ForestName*-Zone, wobei *ForestName* der Name der Stammdomäne ist. Merken Sie sich die Subdomäneneinträge.

4 Identifizieren Sie die *ForestName*-Zone. Merken Sie sich die Subdomäneneinträge.

5 Um die DNS-Integration einer Zone zu überprüfen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf die betreffende Zone, und wählen Sie EIGENSCHAFTEN aus.
2. In der Registerkarte ALLGEMEIN finden Sie alle notwendigen Informationen.

6 Um die Rolle des Anmeldedienstes nachzuvollziehen, können Sie die Protokolldatei `Netlogon.dns` öffnen. Gehen Sie hierfür so vor:

1. Öffnen Sie den Windows Explorer.
2. Gehen Sie in das Verzeichnis `%SystemRoot%\System32\config`, und öffnen Sie die Datei `Netlogon.dns` mit Hilfe des Editors oder mit einem ähnlichen Textprogramm.

Überprüfen der Antwortbereitschaft eines DNS-Servers

Mit dem Tool `nslookup` überprüfen Sie die Namensauflösung.

Voraussetzungen

Besondere Vorkenntnisse benötigen Sie nicht. Für diese Übung brauchen Sie lediglich Folgendes:

- Einen DNS-Server

Durchführung und Aufgabenstellung

Um die Antwortbereitschaft eines DNS-Servers zu prüfen, verwenden Sie das Befehlszeilenprogramm `nslookup`, indem Sie folgende Syntax beachten:

```
nslookup IP_Adresse_des_Servers 127.0.0.1
```

Hierbei ist *IP_Adresse_des_Servers* die IP-Adresse des DNS-Servers, der überprüft werden soll.

1. Lautet die IP-Adresse 192.168.1.1, geben Sie Folgendes ein:

   ```
   nslookup 192.168.1.1 127.0.0.1
   ```

2. Wenn der DNS-Server ordnungsgemäß funktioniert, gibt er den Namen *localhost* zurück.

Überprüfen der DNS-Registrierung für Domänencontroller

Mit dem Tool `nslookup` überprüfen Sie die Namensauflösung.

Voraussetzungen

esondere Vorkenntnisse benötigen Sie nicht. Für diese Übung brauchen Sie lediglich Folgendes:

- Einen Domänencontroller mit einem DNS-Dienst, der eine Active Directory-integrierte Zone hostet.

Durchführung und Aufgabenstellung

SCHRITT FÜR SCHRITT

Geben Sie Folgendes ein:

```
nslookup
```

Danach sind Sie in der Eingabeaufforderung des Programms `nslookup`. Sie sehen dies am »>«-eichen. Damit nur ein bestimmter Ressourceneintragstyp zurückgegeben wird, müssen Sie folgende Syntax verwenden:

```
set q=Ressourceneintragstyp
```

1 Da Sie Ressourceneinträge für die Dienstidentifizierung (SRV-Einträge) überprüfen wollen, müssen Sie Folgendes angeben:

```
set q=srv
```

2 Wenn die Verarbeitung des vorangegangenen Befehls abgeschlossen ist, geben Sie den FQDN des Dienstes an. Hier wird angenommen, dass die Domäne *Berlin.de* heißt.

```
_ldap._tcp.dc._msdcs.Berlin.de
```

3 Lesen Sie die Ausgabe. Wenn die Abfrage erfolgreich gewesen ist, überprüfen Sie die SRV-Ressourceneinträge, um festzustellen, ob alle Domänencontroller der Domäne mit den angegebenen IP-Adressen gültig sind. Schlägt die Abfrage fehl, dann liegt ein Fehler in der dynamischen Aktualisierung des DNS-Servers vor.

```
_ldap._tcp.dc._msdcs.Berlin.de    SRV service location:
    priority        = 0
    weight          = 0
    port            = 389
    svr hostname    = server01.berlin.de
server01.berlin.de  internet address = 192.168.0.201
server01.berlin.de  internet address = 192.168.1.201
```

Listing 2.5: *Auszug aus der Abfrage der SRV-Ressourceneinträge (Beispiel)*

Einrichten von DNS-dynamischen Updates auf DHCP-Clients

Per Voreinstellung aktualisieren Windows Server 2003-basierte, Windows 2000-basierte und Windows XP Professional-Computer ihre A- und PTR-Ressourceneinträge automatisch. Hierbei setzt sich der FQDN aus dem Hostnamen und dem primären DNS-Suffix zusammen. Nach dem Absolvieren der folgenden Übung werden Sie die dynamische Registrierung auf einem Clientcomputer verändern können.

Voraussetzungen

Sie benötigen die folgenden Vorkenntnisse:

- Grundkenntnisse

Für diese Übung benötigen Sie:

- Einen Windows 2000/XP- oder Windows 2000 Server- oder einen Windows Server 2003-Computer

Durchführung und Aufgabenstellung

SCHRITT FÜR SCHRITT

Beachten Sie, dass für das erfolgreiche Durchführen der Übung der DHCP-Clientdienst notwendig ist.

Sie müssen folgende Schritte durchführen:

1. Klicken Sie auf START, dann auf SYSTEMSTEUERUNG und auf NETZWERKVERBINDUNGEN.
2. Anschließend wählen Sie diejenige Netzwerkverbindung aus, die Sie konfigurieren wollen (den lokalen Netzwerkadapter im betreffenden Subnetz). Klicken Sie auf die Schaltfläche EIGENSCHAFTEN.
3. In dem Register ALLGEMEIN wählen Sie INTERNETPROTOKOLL (TCP/IP) aus.
4. Klicken Sie auf die Schaltfläche EIGENSCHAFTEN.
5. Klicken Sie auf ERWEITERT.
6. In dem Register DNS finden Sie das Kontrollkästchen mit der Beschriftung *Adressen dieser Verbindung in DNS registrieren*. Hiermit wird festgelegt, dass der vollständige Name, der in der SYSTEMSTEUERUNG unter SYSTEM eingegeben wurde, zur direkten dynamischen Registrierung (A- und PTR-Record) verwendet wird. Der Eintrag *DNS-Suffix dieser Verbindung in DNS Registrierung verwenden* ist per Default nicht aktiviert.
7. Klicken Sie den Kontrollkästchen-Eintrag *DNS-Suffix dieser Verbindung in DNS Registrierung verwenden* an, und aktivieren Sie dieses mit einem Haken. Die Registrierung besteht zusätzlich zur DNS-Registrierung aus dem vollständigen Computernamen, wie er in der SYSTEMSTEUERUNG unter SYSTEM festgelegt wurde. Wenn der DHCP-Server so konfiguriert ist, dass er DNS-Ressourceneinträge auf die Clientanfrage verarbeitet, wird der Client folgende Einträge auf dem DNS-Server registrieren:

- Einen A-Ressourceneintrag, der sich aus dem verbindungsspezifischen DNS-Suffix (nicht zwangsläufig das primäre DNS-Suffix) und dem Hostnamen des Computers zusammensetzt.
- Einen A-Ressourceneintrag, der sich aus dem primären DNS-Suffix und dem primären Hostnamen des Computers zusammensetzt
- Einen PTR-Ressourceneintrag (PTR-Record)

8 Damit der Client keine Anfragen mehr zur DNS-Registrierung sendet, deaktivieren Sie den Eintrag *Adressen dieser Verbindung in DNS registrieren*.

2.4.4 Übungen für Fortgeschrittene

Da der DNS-Dienst in das Active Directory eingebunden ist, korrespondieren viele Einstellungen auch mit denen im Active Directory. Für diese Übungen wird ein umfangreiches Wissen über die Active Directory vorausgesetzt. Dennoch geht es hier um die Konfiguration des DNS-Servers (und nicht von Active Directory).

Eine domänenweite _msdcs.ForestName-Zone in eine gesamtstrukturweite DNS-Anwendungsverzeichnispartition ändern

Unser Ziel ist es, sekundäre Zonen in den untergeordneten Domänen zu entfernen.

Voraussetzungen

Sie benötigen die folgenden Vorkenntnisse:

- Kenntnisse über DNS-Server
- Grundkenntnisse über den Aufbau einer Active Directory-Domäne

ür diese Übung benötigen Sie:

- Einen Windows Server 2003-basierten Domänencontroller mit einem DNS-Dienst, der Active Directory-integrierte Zonen hostet.
- Für die Übung müssen Sie Mitglied der Gruppe *DnsAdmins* oder einer anderen administrativen Sicherheitsgruppe sein. Alternativ kann Ihnen jedoch auch die Delegation zugesprochen worden sein.
- Wenn Ihr Anmeldekonto nicht Mitglied einer der o.g. Gruppen ist, Sie aber über ein entsprechendes Zugriffskonto verfügen, können Sie mit dem Secondary Logon Service bzw. mit dem `Runas.exe`-Kommando die DNS-Konsole starten.

Durchführung

SCHRITT FÜR SCHRITT

1 Klicken Sie in der DNS-Konsole mit der rechten Maustaste auf die *_msdcs.ForestName*-Zone (hier auch *_msdcs.berlin.de* genannt), und wählen Sie EIGENSCHAFTEN aus.

2 Im Register ALLGEMEIN erkennen Sie die Replikation. In *Abbildung 2.23* sehen Sie zum Beispiel die Voreinstellung nach der Installation des ersten Domänencontrollers. Die

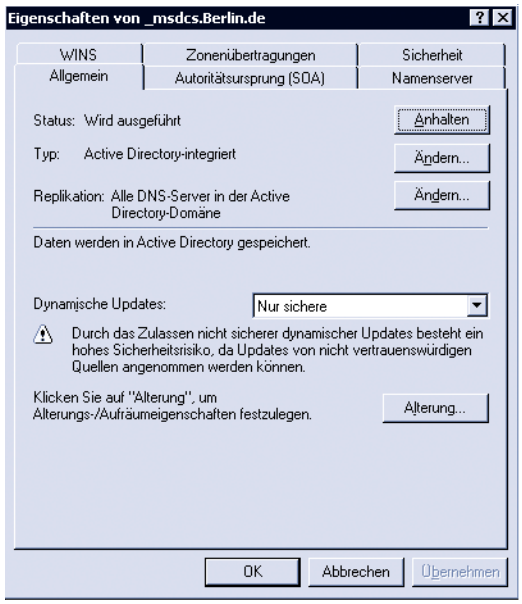


Abbildung 2.23: *Eigenschaften der _msdcs.ForestName-Zone*

3 Gehen Sie auf die Schaltfläche ÄNDERN, wenn die Replikation nur DNS-Server in der Domäne betrifft. Falls der Replikationstyp bereits eine gesamtstrukturweite Replikation unterstützt, fahren Sie mit Schritt 5 fort.

4 Wählen Sie die Option *Auf allen DNS-Servern in der Active Directory-Gesamtstruktur »Domänenname«* (hier *Berlin.de*) aus.

Abbildung 2.24: *Ändern des Bereichs für die Zonenreplikation*

5 Falls Sie sekundäre *_msdcs.ForestName*-Zonen in Ihren untergeordneten Domänen haben, können Sie diese nun löschen. Klicken Sie hierfür mit der rechten Maustaste auf die entsprechende sekundäre Zone, und wählen Sie die Schaltfläche LÖSCHEN aus.

Migrieren einer Windows 2000-_msdcs-Subdomäne zu einer Windows Server 2003-Zone, die auf einer gesamtstrukturweiten Anwendungsverzeichnispartition gespeichert ist

Die Übung basiert auf der Annahme, dass Sie eine Active Directory-Stammdomäne (Root orest Domain) während der Aktualisierung eines Windows 2000 Servers erstellt haben. Die ei Windows 2000 Server bestehende Stammdomäne bleibt somit erhalten. Des Weiteren sind alle Domänencontroller auf Windows Server 2003 aktualisiert bzw. migriert worden.

Voraussetzungen und Lernziele

Sie benötigen folgende Vorkenntnisse:

- Kenntnisse über DNS
- Kenntnisse über Domänenstrukturen
- Kenntnisse über Betriebsmaster

Was lernen Sie?

- Replizieren von DNS-Anwendungsverzeichnispartitionen
- Identifizieren eines Domänennamen-Betriebsmasters
- Erstellen einer primären Zone

ür diese Übung benötigen Sie folgende Computer:

- Einen Windows 2000 Server-basierten Domänencontroller, der zu einem Windows Server 2003-Domänencontroller aktualisiert wurde. Auf dem Domänencontroller befindet sich eine Active Directory-integrierte Zone.
- Mindestens einen Domänencontroller mit DNS-Server für eine Subdomäne (untergeordnete Domäne).

Aufgabenstellung

. Alle primären DNS-Server in der Gesamtstruktur erhalten in den Netzwerkeigenschaften die IP-Adresse eines einzigen Stammdomänencontrollers.

. Erstellen einer *_msdc*-Zone für die Active Directory-Stammdomäne.

. Erstellen einer *_msdcs.ForestName*-Zone in einer gesamtstrukturweiten Anwendungsverzeichnispartition, wobei *ForestName* der von Ihnen gewählte Name der Stammdomäne ist. Der Stammdomänenname kann zum Beispiel *Berlin.de* heißen.

. Starten einer Replikation.

. Umkehren von Schritt 1. Zurückstellen der Netzwerkeigenschaften aller Domänencontroller.

Durchführung

SCHRITT FÜR SCHRITT

Die folgenden Schritte sind hierfür notwendig:

1 Auf allen Domänencontrollern in der Gesamtstruktur müssen Sie die Netzwerkverbindungskonfigurationen so verändern, dass sie nur auf einen DNS-Server zeigen. Dieser DNS-Server wird der bevorzugte DNS-Server. Melden Sie sich auf jedem dieser Server an, und führen Sie folgende Schritte durch:

1. Klicken Sie auf START, dann auf SYSTEMSTEUERUNG und auf NETZWERKVERBINDUNGEN.
2. Anschließend wählen Sie diejenige Netzwerkverbindung aus, die Sie konfigurieren müssen (lokaler Netzwerkadapter im betreffenden Subnetz). Klicken Sie auf EIGENSCHAFTEN.
3. In dem Register ALLGEMEIN wählen Sie *Internetprotokoll (TCP/IP)* aus.
4. Klicken Sie auf EIGENSCHAFTEN.
5. In dem Register ALLGEMEIN finden Sie den Eintrag für den bevorzugten DNS-Server. Notieren Sie sich die DNS-Server-IP-Adresse.
6. In dem Eingabefeld BEVORZUGTER DNS-SERVER geben Sie die IP-Adresse des DNS-Servers ein, der der DNS-Server der Stammdomäne und Domänencontroller ist.
7. Bestätigen Sie die Eingabe mit OK.

Sie müssen alle untergeordneten Domänencontroller mit der IP-Adresse eines einzigen Stammdomänencontrollers konfigurieren. Der Zweck der Übung besteht darin, dass alle Subdomänencontroller ihre Ressourceneinträge zu der Zone *_msdcs.ForestName* kopieren!

2 Nachdem die untergeordneten DNS-Server (alle in der Gesamtstruktur!) den Stammdomänencontroller als bevorzugten DNS-Server eingetragen haben, melden Sie sich mit einem administrativen Konto, das Mitglied der Gruppe *Organisations-Admins* ist, auf dem Stammdomänencontroller an. Der Stammdomänencontroller muss Windows Server 2003-basiert sein.

3 Überprüfen Sie, ob der Server die FSMO-Rolle *Domänennamen-Betriebsmaster* besitzt. Hierfür gehen Sie wie folgt vor:

1. Klicken Sie auf START, dann auf VERWALTUNG und anschließend auf ACTIVE DIRECTORY-DOMÄNEN UND -VERTRAUENSSTELLUNGEN.
2. Sie klicken auf den Knoten ACTIVE DIRECTORY-DOMÄNEN UND -VERTRAUENSSTELLUNGEN mit der rechten Maustaste und wählen aus dem Kontextmenü BETRIEBSMASTER aus.
3. In dem Dialogfenster BETRIEBSMASTER vergewissern Sie sich, dass der Stammdomänencontroller die Rolle des *Domänennamen-Betriebsmasters* hat. Falls dies nicht der Fall sein sollte, ändern Sie die Rolle wie gewünscht.

4 Überprüfen Sie, dass alle DNS-Server die *_msdcs.ForestName*-Subdomäne in primären Zonen hosten. Gehen Sie hierfür wie folgt vor:

1. Klicken Sie auf START, dann auf VERWALTUNG und anschließend auf DNS.
2. Identifizieren Sie die primäre Zone der Subdomäne, und klicken Sie diese an.
3. Identifizieren Sie die *_msdcs.ForestName*-Subdomäne, wobei *ForestName* der Name der Stammdomäne ist (zum Beispiel *Berlin.de)*.

5 Erstellen Sie eine neue Forward-Lookupzone auf dem DNS-Server, der sich auf dem Domänencontroller der Stammdomäne befindet. Gehen Sie so vor:

1. Klicken Sie auf START, dann auf VERWALTUNG und anschließend auf DNS.
2. Wählen Sie den Knoten FORWARD-LOOKUPZONE mit der rechten Maustaste aus, und wählen Sie *Neue Zone*.
3. Ein Konfigurationsassistent hilft Ihnen bei der Erstellung: Erstellen Sie eine primäre Zone, indem Sie die Option auswählen und mit WEITER bestätigen. Achten Sie darauf, dass Sie das Feld *Die Zone in Active Directory speichern ...* mit einem Häkchen markiert haben!
4. In dem Dialogfenster *Active Directory Zonenreplikationsbereich* wählen Sie aus, wie die Zonendaten repliziert werden. Wählen Sie folgendes Optionsfeld: *Auf allen DNS-Servern in der Active Directory-Gesamtstruktur »ForestName«*. Bestätigen Sie die Eingabe mit WEITER.
5. Das nächste Dialogfenster fragt Sie nach dem Namen der Zone. Geben Sie *_msdcs.ForestName* zum Beispiel *Berlin.de* an. Quittieren Sie die Eingabe mit WEITER.
6. Wählen Sie, wie voreingestellt, *Nur sichere dynamische Updates zulassen* aus und bestätigen Sie mit WEITER.
7. Bestätigen Sie das letzte Dialogfenster mit FERTIG STELLEN.

6 Die neue Zone wird erstellt, und der NetLogon-Dienst (Anmeldedienst) füllt diese mit den Ressourceneinträgen des Stammdomänencontrollers. Des Weiteren findet eine Replikation statt. Sie können die Replikation allerdings auch manuell forcieren, indem Sie beispielsweise (bei installierten Support Tools) Folgendes in die Eingabeaufforderung eingeben:

```
repadmin /syncall
```

7 Nachdem alle Verzeichnispartitionen synchronisiert sind, können Sie die alte *_mscds-Subdomäne* löschen. Dieser Schritt ist nicht obligatorisch, er dient lediglich dazu, den DNS-Datenbestand zu straffen. Sollten Sie die Subdomäne beibehalten, wird das keinen Schaden im System anrichten.

1. Sie öffnen die DNS-Verwaltungskonsole.
2. In dem Konsolenbaum erweitern Sie diejenige Zone, die die *_msds-Subdomäne* enthält.
3. Löschen Sie diese Zone über das Kontextmenü mit der rechten Maustaste.

8 Der letzte Schritt macht den ersten wieder rückgängig. Tragen Sie in den Eigenschaften der betreffenden Netzwerkkarten wieder die ursprünglichen IP-Adressen für den bevor-

2.4.5 Antworten zu den Wiederholungsfragen

Hier finden Sie die Antworten zu den Aufgaben aus *Kapitel 2.4.1*.

1. Wie unterscheidet sich ein Namensraum von einer Microsoft-Domäne?

Antwort: Eine Microsoft-Domäne ist eine logische Zusammenfassung von Computern, wobei ein Microsoft-Domänencontroller mit Hilfe von Computerkonten bestimmt, wer sich an der Domäne anmelden darf. Die Verwaltung obliegt einem Administrator der Domäne. Die Domäne bekommt einen Namen, der sich nach der Schreibweise für DNS-Namen richtet. Somit richtet sich der Name der Domäne nach dem Namensraum.

Der Namensraum ist eine hierarchische baumartige Struktur von Namen. Jeder Name bezeichnet eine Domäne bzw. Zone. Die Schreibweise hierfür ist ein vollqualifizierter Domänenname (FQDN). Ein Beispiel für einen Namensraum sind *microsoft.com* und alle untergeordneten Domänen wie *boston.microsoft.com* oder *new-york.microsoft.com* usw.

2. Warum ist die Planung des DNS-Namensraums so wichtig für das Active Directory?

Antwort: Eine Änderung des Namensraums kann u.U. nur mit extrem hohem Aufwand (komplette Neuinstallation) durchgeführt werden. Die Umbenennung einer Stammdomäne ist nur dann möglich, wenn Sie den vollständigen Active Directory-Namensraum bzw. die Gesamtstruktur (Forest) umbenennen.

3. Wer entscheidet bei der Planung des Namensraums?

Antwort: Es existieren zwei Arten von Namensräumen: Externe und interne Namensräume. Für die externen Namensräume sind Internetorganisationen wie die IANA verantwortlich, während für den internen Namensraum die betreffenden Organisationen zuständig sind. Anders ausgedrückt: Sie als Anwender können Ihren internen Namensraum so gestalten, wie Sie möchten.

4. Welche besonderen Features hat ein Windows Server 2003-DNS-Server?

Antwort: Folgende Leistungsmerkmale charakterisieren einen Microsoft DNS-Server auf Windows Server 2003-Basis:

- Unterstützt SRV-Einträge
- Sichere und nicht sichere dynamische Aktualisierung
- Inkrementelle Zonenübertragung
- WINS-Integration
- Bedingte Weiterleitung
- Active Directory-integrierte Zonen
- Aufräumvorgänge für alte Einträge

5. Können für das Active Directory auch Nicht-Windows-DNS-Server verwendet werden?

Antwort: Ja. Es muss ein BIND-Server Version 4.9.7 oder höher verwendet werden. Die aktuelle Version 9 unterstützt alle wesentlichen Features des Windows Server 2003 bis auf die Aufräumvorgänge und bis auf diejenigen Vorgänge, die sich auf eine Active Directory-Integration eziehen. Darunter fallen die sichere dynamische Aktualisierung und eine WINS-Integration.

6. Wie verhält es sich mit Windows NT- und Windows 98-Clients hinsichtlich einer dynamischen Aktualisierung?

Antwort: Es besteht die Möglichkeit, für Windows NT 4.0- und Windows 98-Clients die dynamische Aktualisierung einzustellen. Gleiches gilt auch für die Verwendung von DHCP Dynamic Host Configuration Protocol).

7. Welche Replikationsmechanismen gibt es?

Antwort: Normale Replikationsmechanismen erlauben Zonenübertragungen zu Computern, die Sie bestimmen können.

Wenn Sie einen sekundären DNS-Server verwenden, wird eine »NurLesen-Kopie« einer primären Zone generiert. Auch findet eine Zonenübertragung statt, jedoch nur in einer Richtung.

Wenn Sie eine Active Directory-integrierte Zone verwenden, können Sie zwischen folgenden Replikationsoptionen auswählen:

- Alle DNS-Server in der Active Directory-Gesamtstruktur
- Alle DNS-Server in einer angegebenen Active Directory-Domäne
- Alle Domänencontroller in der Active Directory-Domäne
- Alle Domänencontroller, die im Replikationsbereich einer Anwendungsverzeichnispartition angegeben wurden

Mehr zu diesem Thema können Sie in *Kapitel 2.2.7* nachlesen.

2.4.6 Antworten zu den Übungen

Hier finden Sie die Antworten zu den Aufgaben in den *Kapiteln 2.4.3* und *2.4.4*. Zur Übersicht ist die Aufgabenstellung hier noch einmal aufgeführt.

Überprüfen der DNS-Konfiguration

iel: Nach der Installation des ersten Domänencontrollers soll die DNS-Server-Konfiguration überprüft werden.

Vorgang: Sie installieren eine Active Directory-Domäne mit dem *Assistenten zum Installieren von Active Directory*. Sie lassen ihn alle Einstellungen für das Active Directory vornehmen.

Die Domäne wurde *Berlin.de* genannt. Sie ist in einem Subnetz 192.168.0.0/24 installiert.

Überprüfen Sie folgende Sachverhalte:

1. Welche Zonen und Zonentypen werden erstellt?

Antwort: Wenn Sie sich alle Zonen anzeigen lassen wollen, müssen Sie im Menü ANSICHT den Eintrag *Erweiterte Ansicht* auswählen.

Forward-Lookupzone	Beschreibung
`msdcs.Berlin.de`	Wird zur Kompatibilität mit Windows 2000 Server benötigt. Die _msdcs.ForestName-Zone ist in der gesamtstrukturweiten Anwendungsverzeichnispartition gespeichert. Es werden keine A-Records erstellt. Zonentyp: Active Directory-integriert, primär.
`Berlin.de`	Die eigentliche DNS-Zone. Sie enthält alle benötigten Ressourceneinträge (Record), wie die A-Records des DNS-Servers. Der DNS-Server muss sich zuallererst selbst in die Zone aktualisieren. Zonentyp: Active Directory-integriert, primär.

Tabelle 2.11: *Erstellte Forward-Lookzonen beim Stammdomänencontroller (Forest Root Domain Controller)*

Reverse-Lookupzone	Beschreibung
`0.168.192.in-addr.arpa`	Falls die *Erweiterte Ansicht* nicht ausgewählt wurde, wird die Zone mit *192.168.0.x Subnet* bezeichnet. Zonentyp: Primär (nicht Active Directory-integriert)
`0.in-addr.arpa`	Zwei Einträge für Netzwerk. Keine weiteren Eigenschaften verfügbar.
`127.in-addr.arpa`	Drei Einträge für Localhost. Keine weiteren Eigenschaften verfügbar.
`255.in-addr.arpa`	Drei Einträge für Broadcast. Keine weiteren Eigenschaften verfügbar.

Tabelle 2.12: *Erstellte Reverse-Lookupzonen beim Stammdomänencontroller (Forest Root Domain Controller)*

2. Wie sieht die Replikation der DNS-Zonen aus?

Zone	Beschreibung
`msdcs.Berlin.de`	Alle DNS-Server in der Active Directory-Gesamtstruktur (Grundeinstellung bei Windows 2000 Server)
`Berlin.de`	Alle DNS-Server in der Active Directory-Gesamtstruktur (Grundeinstellung bei Windows 2000 Server)
`0.168.192.in-addr.arpa`	Keine, da nicht Active Directory-integriert

Tabelle 2.13: *Replikationseinstellungen bei den neu erstellten Zonen.*

3. Welche Rolle spielt der Anmeldedienst bei der Konfiguration der Domänencontroller?

Antwort: Der Anmeldedienst (Logon Service) füllt die Zonendateien mit Daten.

4. Welche SRV-Record-Typen gibt es, und wie hängen diese mit einem Domänencontroller zusammen?

Dienstidentifizierung (SRV)	Standardwert	Beschreibung
_gc	[0][100][3268] server01.berlin.de.	Dient zum Finden eines Globalen Katalogservers. Der Port 3268 wird verwendet. Ist der Domänencontroller kein Globaler Katalogserver, benötigt er auch keine _gc-Dienstidentifizierung.
_kerberos	[0][100][88] server01.berlin.de.	Erlaubt Computern, das Kerberos-Schlüsselverteilungscenter (KDC-Server) zu finden. Alle Domänencontroller, die den Kerberos-Dienst anbieten, registrieren diesen Namen. Der KDC-Server ist nicht notwendigerweise ein Windows Server 2003-Domänencontroller. Bei dem Dienst handelt es sich um ein RFC 1510-kompatible-Kerberos Version 5-KDC (Key Distribution Center). Der Port 88 wird verwendet.
_kpasswd	[0][100][464] server01.berlin.de.	Ermöglicht es einem Client, einen Domänencontroller zu finden, auf dem ein Kerberos-Schlüsselverteilungscenter (KDC) ausgeführt wird. Alle Windows NT-Domänencontroller, auf denen der Kerberos KDC-Dienst ausgeführt wird, registrieren diese SRV. Der Port 464 wird verwendet.
_ldap	[0][100][389] server01.berlin.de.	Erlaubt Computern, den Domänencontroller zu finden. Der Port 389 wird verwendet.

abelle 2.14: *SRV-Records mit Standardwerten*