



DNS EINRICHTEN

Luis Lüscher M123

Inhalt

Linux Centos DHCP einrichten	2
Windows DNS einrichten.....	7
Vorbereitung	7
Installation.....	7
Konfiguration.....	8
Testen	12
Ubuntu DNS einrichten	Fehler! Textmarke nicht definiert.

Linux Centos DHCP einrichten

```
[root@sv01 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:c2:13:23 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global noprefixroute dynamic enp0s3
        valid_lft 85686sec preferred_lft 85686sec
    inet6 fe80::aef9:2bb1:219e:aaab/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Durch die Eingabe von `ip a` finden wir heraus wie die Netzwerkkarte heisst. In diesem Fall **enp0s3**.

```
[root@sv01 ~]# nano /etc/sysconfig/network-scripts/ifcfg-enp0s3
```

Danach öffnen wir die Konfigurationsdatei der Netzwerkkarte über oben stehenden Command. Wichtig ist das man die richtige Konfigurationsdatei öffnet (siehe gelbe Markierung).

GNU nano 2.3.1	Datei: /etc/sysconf	GNU nano 2.3.1	Datei: /etc/sysconf
TYPE="Ethernet"		TYPE="Ethernet"	
PROXY_METHOD="none"		PROXY_METHOD="none"	
BROWSER_ONLY="no"		BROWSER_ONLY="no"	
BOOTPROTO="dhcp"		BOOTPROTO="static"	
DEFROUTE="yes"		DEFROUTE="yes"	
IPV4_FAILURE_FATAL="no"		IPV4_FAILURE_FATAL="no"	
IPV6INIT="yes"		IPV6INIT="yes"	
IPV6_AUTOCONF="yes"		IPV6_AUTOCONF="yes"	
IPV6_DEFROUTE="yes"		IPV6_DEFROUTE="yes"	
IPV6_FAILURE_FATAL="no"		IPV6_FAILURE_FATAL="no"	
IPV6_ADDR_GEN_MODE="stable-privacy"		IPV6_ADDR_GEN_MODE="stable-privacy"	
NAME="enp0s3"		NAME="enp0s3"	
UUID="d80bdeb9-2d7c-4114-a4e1-60199e23c3c1"		UUID="d80bdeb9-2d7c-4114-a4e1-60199e23c3c1"	
DEVICE="enp0s3"		DEVICE="enp0s3"	
ONBOOT="yes"		ONBOOT="yes"	

Nun müssen wir unter **BOOTPROTO** den nachfolgenden Wert **«dhcp»** auf **«static»** ändern.

```
IPADDR="192.168.100.21"
NETMASK="255.255.255.0"
GATEWAY="192.168.100.1"
DNS1="1.0.0.1"
DNS2="1.1.1.1"
DNS3="8.8.8.8"
```

Nachher müssen wir die Datei noch um folgende Daten ergänzen. Durch diese Ergänzungen erhält die Netzwerkkarte eine fixe IP-Adresse

```
IPADDR=`192.168.100.21`
NETMASK=`255.255.255.0`
GATEWAY=`192.168.100.1`
DNS1=`1.0.0.1`
DNS2=`1.1.1.1`
DNS3=`8.8.8.8`
```

```
[root@sv01 ~]# systemctl restart network
```

Danach starten wir die Netzwerkkarte neu. Durch oben stehen Command.

```
[root@sv01 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
    link/ether 08:00:27:c2:13:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.21/24 brd 192.168.100.255 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::aef9:2bb1:219e:aaab/64 scope link
        valid_lft forever preferred_lft forever
```

Wenn wir nun erneut **ip a** eingeben, sehen wir dass unsere Netzwerkkarte **enp0s3** nun die von uns definierte IP-Adresse erhält.

```
[root@sv01 ~]# hostnamectl
```

Mit der Eingabe von **hostnamectl** finden wir den **static hostname** heraus.

```
[root@sv01 ~]# hostnamectl
Static hostname: sv01.altos.local
Icon name: computer-vm
Chassis: vm
Machine ID: 3bb681d9038d41a381f382f22c77233d
Boot ID: 337dc659899e413b9ae03d6dc237a648
Virtualization: kvm
Operating System: CentOS Linux 7 (Core)
CPE OS Name: cpe:/o:centos:centos:7
Kernel: Linux 3.10.0-957.el7.x86_64
Architecture: x86-64
```

Der **static hostname** ist hier **rot** markiert.

```
[root@sv01 ~]# yum install bind bind-utils
```

Nun installieren wir das DNS Service Package mit folgenden Command.

Yum install bind bind-utils

```
[root@sv01 ~]# nano /etc/named.conf
```

Nun öffnen wir **/etc/named.conf** mit einem Editor. Dies ist die Konfigurationsdatei des DNS Server.

```
options {
    listen-on port 53 { 127.0.0.1;192.168.100.21; };
    listen-on-v6 port 53 { ::1; };
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    recursing-file "/var/named/data/named.recursing";
    secroots-file "/var/named/data/named.secroots";
    allow-query { localhost;any; };
}
```

Unter **options** schreiben wir nach dem Semikolon unsere fixe IP-Adresse (Zwingend hier am nede der Ip-Adresse das Semikolon nicht vergessen. Unter **allow-query** schreiben wir nach dem Semikolon **any**. Hier ebenfalls nicht das Semikolon vergessen!

```
[root@sv01 ~]# systemctl start named
```

Mit obenstehenden Command starten wir den Named Service.

```
[root@sv01 ~]# sudo systemctl enable named
```

Mit obenstehenden Command aktivieren wir den Named Service.

```
[root@sv01 ~]# sudo systemctl status named
```

Mit diesem Command kann man nun den Status des Named Service einsehen. Nach kurzer Ladezeit erscheint folgendes.

```
[root@sv01 ~]# sudo systemctl status named
■ named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
   Active: active (running) since Son 2019-06-30 20:05:04 CEST; 1min 28s ago
     Main PID: 21007 (named)
    CGroup: /system.slice/named.service
            └─21007 /usr/sbin/named -u named -c /etc/named.conf

Jun 30 20:05:08 sv01.altos.local named[21007]: network unreachable resolving './NS/IN': 2001:5...#53
Jun 30 20:05:11 sv01.altos.local named[21007]: network unreachable resolving './DNSKEY/IN': 20...#53
Jun 30 20:05:11 sv01.altos.local named[21007]: network unreachable resolving './NS/IN': 2001:5...#53
Jun 30 20:05:11 sv01.altos.local named[21007]: network unreachable resolving './DNSKEY/IN': 20...#53
Jun 30 20:05:11 sv01.altos.local named[21007]: network unreachable resolving './NS/IN': 2001:d...#53
Jun 30 20:05:12 sv01.altos.local named[21007]: network unreachable resolving './DNSKEY/IN': 20...#53
Jun 30 20:05:12 sv01.altos.local named[21007]: network unreachable resolving './NS/IN': 2001:7...#53
Jun 30 20:05:14 sv01.altos.local named[21007]: network unreachable resolving './DNSKEY/IN': 20...#53
Jun 30 20:05:14 sv01.altos.local named[21007]: network unreachable resolving './NS/IN': 2001:5...#53
Jun 30 20:05:14 sv01.altos.local named[21007]: managed-keys-zone: Unable to fetch DNSKEY set '...out
Hint: Some lines were ellipsized, use -l to show in full.
```

Wenn dies so erscheint hast du alles richtig gemacht. Ansonsten würde ich empfehlen nochmal die Konfigurationsdatei durchzugehen und nach fehlenden Semikolons nachzuschauen.

```
[root@sv01 ~]# firewall-cmd --permanent --add-port=52/tcp
success
[root@sv01 ~]# firewall-cmd --permanent --add-port=52/udp
success
```

Der nächste Schritt wäre die Firewall anzupassen. Dies jeweils für den Port 52 für TCP und UDP.

```
[root@sv01 ~]# firewall-cmd --reload
success
```

Nun lädt man die Firewall neu.

```
[root@sv01 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: ssh dhcpv6-client
  ports: 52/tcp 52/udp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Und durch **firewall-cmd --list-all** kann man nachschauen ob unter **ports** die beiden Ports angezeigt werden.

```
[root@sv01 ~]# nano /etc/named.conf
```

Nun öffnen wir die Konfigurationsdatei mit einem Editor.

```
zone "altos.local" IN {
type master;
file "forward.altos.local";
allow-update { none; };
};

zone "1.168.192.in-addr.arpa" IN {
type master;
file "reverse.altos.local";
allow-update { none; };
};
```

Nun gehen wir beim File ganz runter und ergänzen nach der zone `` die Datei um folgenden Zonen. Zu Schluss speichern wir die Datei.

```
[root@sv01 ~]# cd /var/named/
```

Nun wechseln wir ins /var/named/ Verzeichnis

```
[root@sv01 named]# cp named.localhost forward.altos.local
```

Wir kopieren das default named.localhost und nennen es gleichzeitig forward.altos.local, so wie wir es vorhin in der Konfigurationsdatei bei den Zonen genannt haben.

```
[root@sv01 named]# nano forward.altos.local
```

Nun öffnen wir das kopierte File mit einem Editor.

```
$TTL 1D
@      IN SOA  @ sv01.altos.local. root.altos.local. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum
@      IN     NS      sv01.altos.local.
@      IN     A       192.168.100.21
server IN     A       192.168.100.21
host   IN     A       192.168.100.21
desktop IN    A       192.168.100.101
client IN     A       192.168.100.101
```

Nun Ergänzen wir folgende Angaben im File.

```
[root@sv01 named]# cp forward.altos.local reverse.altos.local
```

Nun kopieren wir das bearbeitete File und nennen es so wie vorhin in der Konfigurationsdatei angegeben.

```
[root@sv01 named]# nano reverse.altos.local
```

Auch diese Datei öffnen wir mit einem Editor.

```
$TTL 1D
@      IN SOA  @ sv01.altos.local. root.altos.local. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum

@      IN      NS      sv01.altos.local.
@      IN      PTR     altos.local.
server IN      A       192.168.100.21
host   IN      A       192.168.100.21
desktop IN     A       192.168.100.101
client IN      A       192.168.100.101
21     IN      PTR     sv01.altos.local.
101    IN      PTR     desktop.altos.local.
```

Hier sind müssen wir die Datei um oben stehende Angaben ergänzen.

```
[root@sv01 named]# ll
insgesamt 24
drwxrwx---. 2 named named  23 30. Jun 20:05 data
drwxrwx---. 2 named named   60 30. Jun 21:05 dynamic
-rw-r-----. 1 root  root  302 30. Jun 21:20 forward.altos.local
-rw-r-----. 1 root  named 2281 22. Mai 2017 named.ca
-rw-r-----. 1 root  named  152 15. Dez 2009 named.empty
-rw-r-----. 1 root  named  152 21. Jun 2007 named.localhost
-rw-r-----. 1 root  named  168 15. Dez 2009 named.loopback
-rw-r-----. 1 root  root   362 30. Jun 21:25 reverse.altos.local
drwxrwx---. 2 named named    6  4. Jun 21:26 slaves
```

Wenn man nun schaut wie es bezüglich der Berechtigungen aussieht sehen wir, dass die beiden von uns erstellten Files immer noch für root bestimmt ist. Dies müssen wir durch folgenden Command verändern.

```
[root@sv01 named]# chown root:named forward.altos.local
[root@sv01 named]# chown root:named reverse.altos.local
```

Den Befehle **chown root:named** führen wir 2 mal durch einmal für die forward Datei und einmal für die reverse Datei.

```
[root@sv01 named]# ll
insgesamt 24
drwxrwx---. 2 named named  23 30. Jun 20:05 data
drwxrwx---. 2 named named   60 30. Jun 21:05 dynamic
-rw-r-----. 1 root  named  302 30. Jun 21:20 forward.altos.local
-rw-r-----. 1 root  named 2281 22. Mai 2017 named.ca
-rw-r-----. 1 root  named  152 15. Dez 2009 named.empty
-rw-r-----. 1 root  named  152 21. Jun 2007 named.localhost
-rw-r-----. 1 root  named  168 15. Dez 2009 named.loopback
-rw-r-----. 1 root  named  362 30. Jun 21:25 reverse.altos.local
drwxrwx---. 2 named named    6  4. Jun 21:26 slaves
```

Wenn wir nun ll sehen wir das die Berechtigung funktioniert hat.

```
[root@sv01 named]# named-checkconf -z /etc/named.conf
```

Nun überprüfen wir ob das Konfigurationsfile richtig konfiguriert ist.

```
[root@sv01 named]# named-checkzone forward /var/named/forward.altos.local
```

Das selbe machen wir beim forward file.

```
[root@sv01 named]# named-checkzone forward /var/named/reverse.altos.local
```

Sowie beim reverse file.

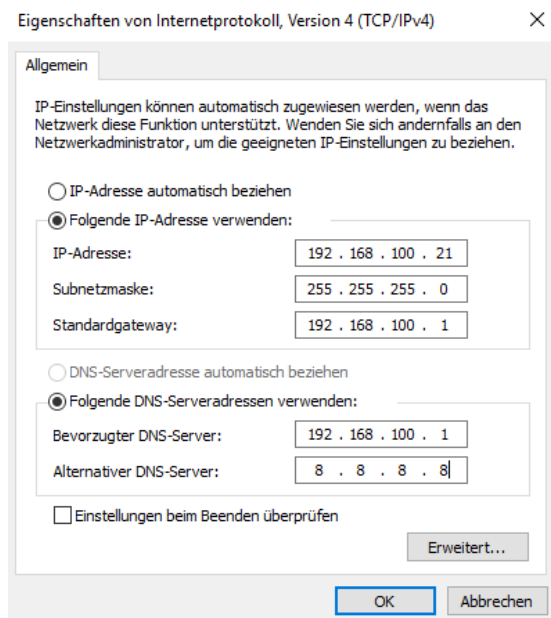
```
[root@sv01 named]# systemctl restart named
```

Danach starten wir den Service neu.

Durch **nslookup IP_ADRESSE** können wir nun sehen ob es funktioniert. Dieser Schritt funktionierte bei mir bei CentOS **nicht**. Der Server konnte ich zwar vom Client aus Pingen jedoch funktionierte nslookup nicht.

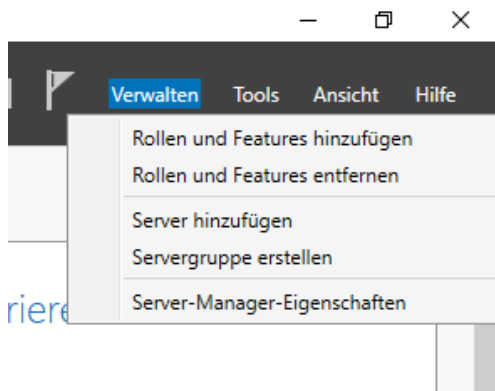
Windows DNS einrichten

Vorbereitung



Installation

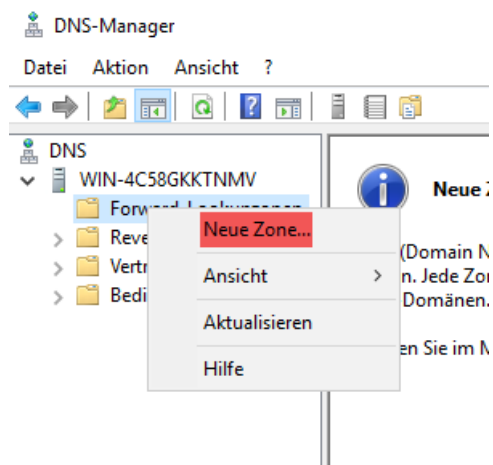
Wir müssen dem Server zuvor noch eine fixe IP-Adresse vergeben. In diesem Fall **192.168.100.21**.



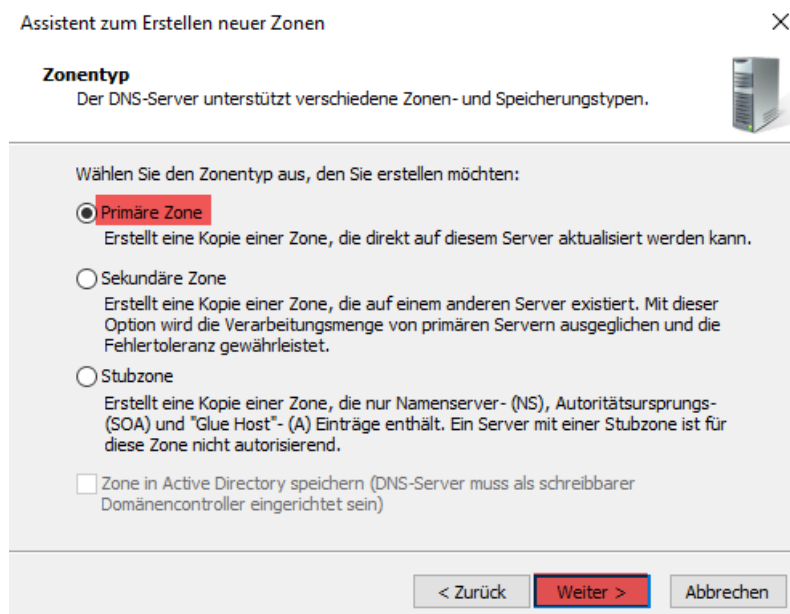
Unter **Verwalten** gehen wir auf **Rollen und Features hinzufügen**. Hier kann man dann DNS auswählen und den Server-Dienst installieren. Danach sollte man den Dienst starten (Suche nach DNS).

Konfiguration

Forward Lookupzone



Den Ordner auf dem der Hostname steht öffnen und dann rechtsklick auf Forward-Lookupzonen
Nachfolgenden auf neue Neue Zone...



Auf «Primäre Zone» klicken und mit «Weiter» bestätigen

Zonenname

Wie lautet der Name der neuen Zone?



Der Zonenname bestimmt den Teil des DNS-Namespace, für den dieser Server autorisierend ist. Normalerweise wird der Firmendomänenname (wie z. B. "microsoft.com") oder ein Teil des Domänennamens (wie z. B. "neuezone.microsoft.com") verwendet. Der Zonenname ist nicht der Name des DNS-Servers.

Zonenname:

< Zurück

Weiter >

Abbrechen

Zonennamen bestimmen in diesem Fall «altos.local».

Zonendatei

Sie können eine neue Zonendatei erstellen, oder Sie können eine Datei von einem anderen DNS-Server kopieren.



Möchten Sie eine Datei für neue Zonen erstellen oder eine vorhandene Datei verwenden, die Sie von einem anderen DNS-Server kopiert haben?

☒ Neue Datei mit diesem Dateinamen erstellen:☐ Vorhandene Datei verwenden:

Vergewissern Sie sich, dass die bestehende Datei in den Ordner %SystemRoot%\system32\dns auf diesem Server kopiert wurde, um die bestehende Datei zu verwenden, und klicken Sie auf "Weiter".

< Zurück

Weiter >

Abbrechen

Der vorgeschlagene Namen kann so bleiben und mit «Weiter» bestätigt werden.

Assistent zum Erstellen neuer Zonen

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

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

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

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

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

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

< Zurück Weiter > Abbrechen

«Dynamische Updates nicht zulassen» auswählen und mit «Weiter» bestätigen.

Assistent zum Erstellen neuer Zonen

Fertigstellen des Assistenten

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

Name: "altos.local"
 Typ: "Primär (Standard)"
 Lookuptyp: "Weiter"
 Dateiname: "altos.local.dns"

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

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

< Zurück Fertig stellen Abbrechen

Dieses Fenster mit «Fertig stellen» bestätigen

Reverse Lookupzone

Nun müssen wir erneut eine **primäre Zone** erstellen.

Assistent zum Erstellen neuer Zonen

Zonentyp
 Der DNS-Server unterstützt verschiedene Zonen- und Speichertypen.

Wählen Sie den Zonentyp aus, den Sie erstellen möchten:

☒ **Primäre Zone**
 Erstellt eine Kopie einer Zone, die direkt auf diesem Server aktualisiert werden kann.

☐ Sekundäre Zone
 Erstellt eine Kopie einer Zone, die auf einem anderen Server existiert. Mit dieser Option wird die Verarbeitungsmenge von primären Servern ausgeglichen und die Fehlertoleranz gewährleistet.

☐ Stubzone
 Erstellt eine Kopie einer Zone, die nur Namensserver - (NS), Autoritätsursprungs- (SOA) und "Glue Host"- (A) Einträge enthält. Ein Server mit einer Stubzone ist für diese Zone nicht autorisierend.

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

< Zurück Weiter > Abbrechen

«IPv4 Reverse-Lookupzone» auswählen und mit «Weiter» bestätigen

Assistent zum Erstellen neuer Zonen

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

Legen Sie fest, ob Sie eine Reverse-Lookupzone für IPv4- oder IPv6-Adressen erstellen möchten.

☒ IPv4 Reverse-Lookupzone

☐ IPv6 Reverse-Lookupzone

< Zurück Weiter > Abbrechen

Hier müssen wir den Netzwerkanteil angeben. Nachher mit «Weiter» bestätigen.

Assistent zum Erstellen neuer Zonen

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

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

☒ Netzwerk-ID:

192.168.100

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

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

☐ Name der Reverse-Lookupzone:

100.168.192.in-addr.arpa

< Zurück Weiter > Abbrechen

Der vorgeschlagene Name kann man stehen lassen und mit «Weiter» bestätigen.

Assistent zum Erstellen neuer Zonen

Zonendatei
Sie können eine neue Zonendatei erstellen, oder Sie können eine Datei von einem anderen DNS-Server kopieren.

Möchten Sie eine Datei für neue Zonen erstellen oder eine vorhandene Datei verwenden, die Sie von einem anderen DNS-Server kopiert haben?

☒ Neue Datei mit diesem Dateinamen erstellen:

100.168.192.in-addr.arpa.dns

☐ Vorhandene Datei verwenden:

Vergewissern Sie sich, dass die bestehende Datei in den Ordner %SystemRoot%\system32\dns auf diesem Server kopiert wurde, um die bestehende Datei zu verwenden, und klicken Sie auf "Weiter".

< Zurück Weiter > Abbrechen

Dynamisches Update


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



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

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

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

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

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

< Zurück

Weiter >

Abbrechen

«Dynamische Updates nicht zulassen» auswählen und mit «Weiter» bestätigen. Am Ende muss man noch den DNS Eintrag für den Server machen.

Testen

☐ DNS-Serveradresse automatisch beziehen

☒ Folgende DNS-Serveradressen verwenden:

Bevorzugter DNS-Server:

Alternativer DNS-Server:

☐ Einstellungen beim Beenden überprüfen

Erweitert...

OK Abbrechen

Auf dem Client muss bei den DNS Einstellungen beim **Bevorzugten DNS-Server** die IP des Server eingeben. In diesem Fall **192.168.100.21**.

Auf dem Client muss man den DNS Cache leeren mit **ipconfig /flushdns**

```
C:\Users\Administrator>ipconfig /flushdns
```

Jetzt muss man auf dem Server in der Forwardlookupzone einen neuen Record machen.

Neuer Host ✕

Name (bei Nichtangabe wird übergeordneter Domänenname verwendet):

Vollqualifizierter Domänenname:

IP-Adresse:

☒ Verknüpften PTR-Eintrag erstellen

Nun pingen wir den Server von Client aus.

```
C:\Users\Administrator>ping server.altos.local

Ping wird ausgeführt für server.altos.local [192.168.100.21] mit 32 Bytes Daten:
Antwort von 192.168.100.21: Bytes=32 Zeit<1ms TTL=128
Antwort von 192.168.100.21: Bytes=32 Zeit<1ms TTL=128
Antwort von 192.168.100.21: Bytes=32 Zeit<1ms TTL=128
Antwort von 192.168.100.21: Bytes=32 Zeit<1ms TTL=128

Ping-Statistik für 192.168.100.21:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
            (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
```

Danach **nslookup 192.168.100.101** um alle Domains abzufragen, die mit dieser IP verbunden sind.

```
C:\Users\Administrator>nslookup 192.168.100.101
Server:      server.altos.local
Address:     192.168.100.21

Name:       test.altos.local
Address:    192.168.100.101
```