



_msdcs Zone gesamtstrukturweit neu anlegen

Ohne DNS funktioniert kein Microsoft Active Directory. Wichtig hierbei ist die `_msdcs` Zone die vor Server 2003 eine untergeordnete Zone war.

Diese Zone wird auch als Standardanwendungs-Verzeichnispartition bezeichnet. Sie enthält Informationen über Dienste des Active Directorys, z.B. Domänencontroller, Globale Kataloge usw.

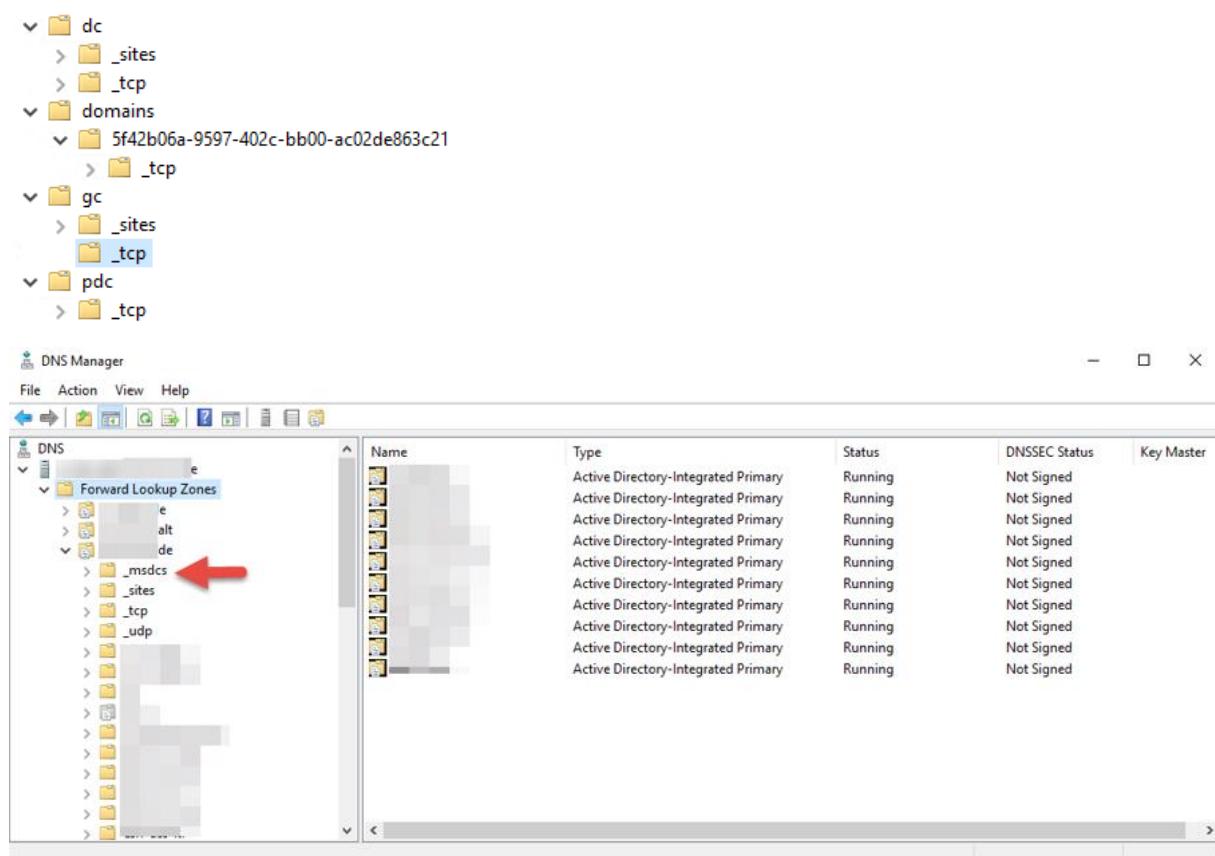
Was passiert, wenn hier ein Fehler vorliegt?

Keine Panik! Alle Einträge lassen sich schnell und zügig wiederherstellen.

Folgende Befehle führen wir dafür nach einander aus:

1. dcdiag /fix
 2. netdiag /fix

Damit werden die Parameter neu geschrieben.



Ab Server 2003 muss die _msdsc Zone direkt unter dem Ordner Forward Lookup Zones angelegt sein/werden. Das betrifft hauptsächlich 2000er Domänen die auf 2003/2008 hochgestuft werden/wurden.

DCPROMO erstellt ab Windows Server 2003 hierfür automatisch eine separate Zone. Das hat den Hintergrund, dass die Informationen der globalen Kataloge der Gesamtstruktur sonst nur in der Zone der Stammdomäne vorhanden wären.

Ein DC/Client in einer Subdomain müsste so immer die Zone der Stammdomäne erreichen können, um einen globalen Katalog zu finden. Wenn diese aus Netzwerkgründen nicht erreichbar ist, hat der DC/Client der Subdomain ein Problem den nächsten verfügbaren globalen Katalog zu finden.



_msdcs Zone gesamtstrukturweit neu anlegen

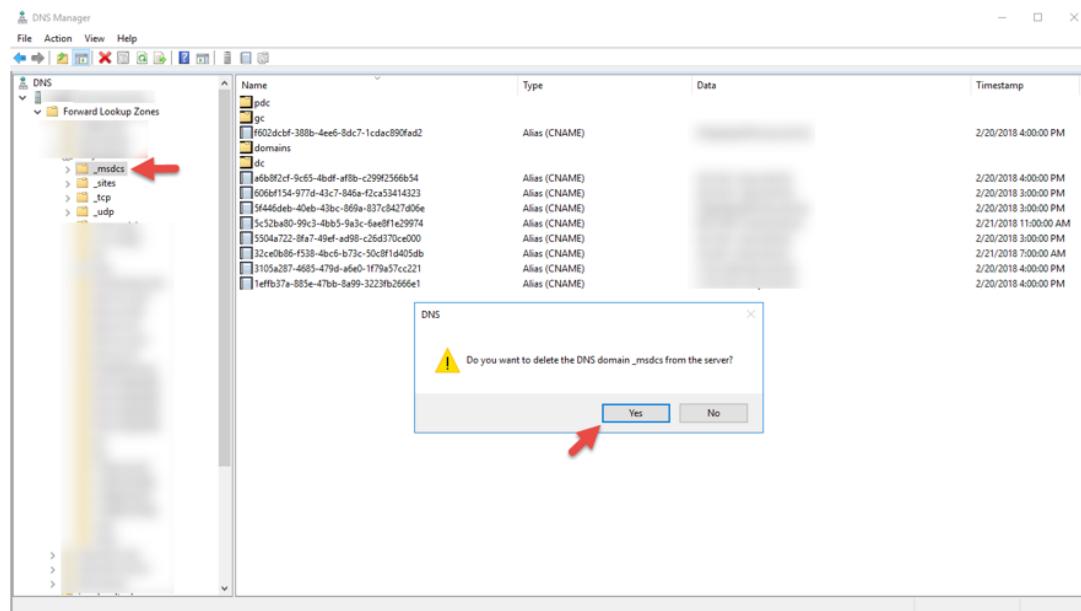
Deshalb wird diese Zone ab Windows Server 2003 als eigenständige Zone eingerichtet und auf alle DCs der Gesamtstruktur repliziert. Damit kennt jeder DC/Client im gesamten Forest automatisch z.B. alle globalen Kataloge.

Ergebnis des BPA falls diese Zone unterhalb einer Subdomain liegt.

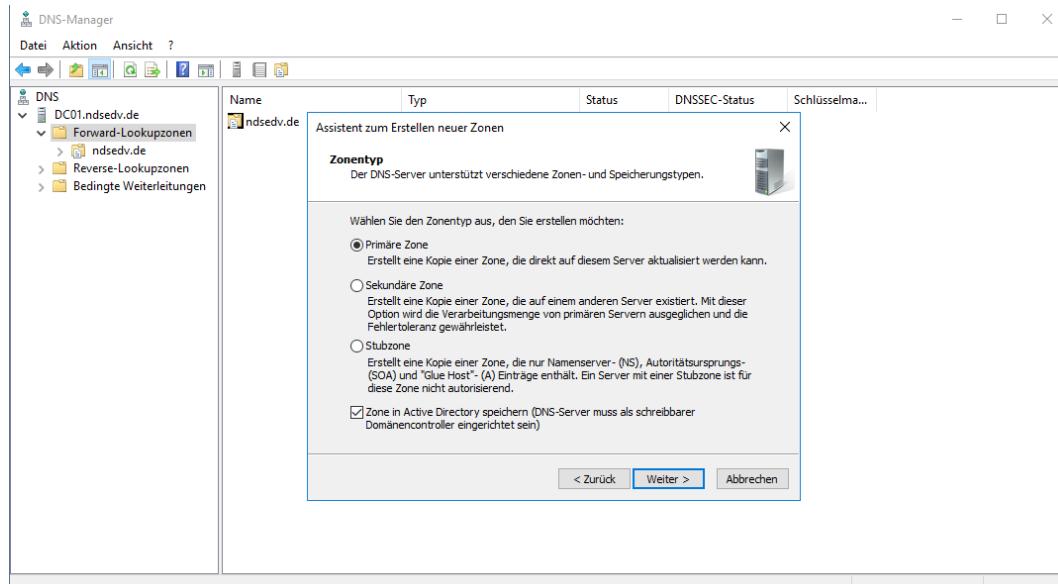
DNS: Zone _msdcs.ndsedv.de is an Active Directory integrated DNS Zone and must be available. Problem: The Active Directory integrated DNS zone _msdcs.ndsedv.de was not found.

Und so gehen wir vor um die Zone _msdcs.ndsedv.de gesamtstrukturweit bereitzustellen:

Löschen der Zone namens _msdcs unterhalb der Domäne ndsedv.de sowie die Forward- und Reverse Lookup Eintrag des DCs.



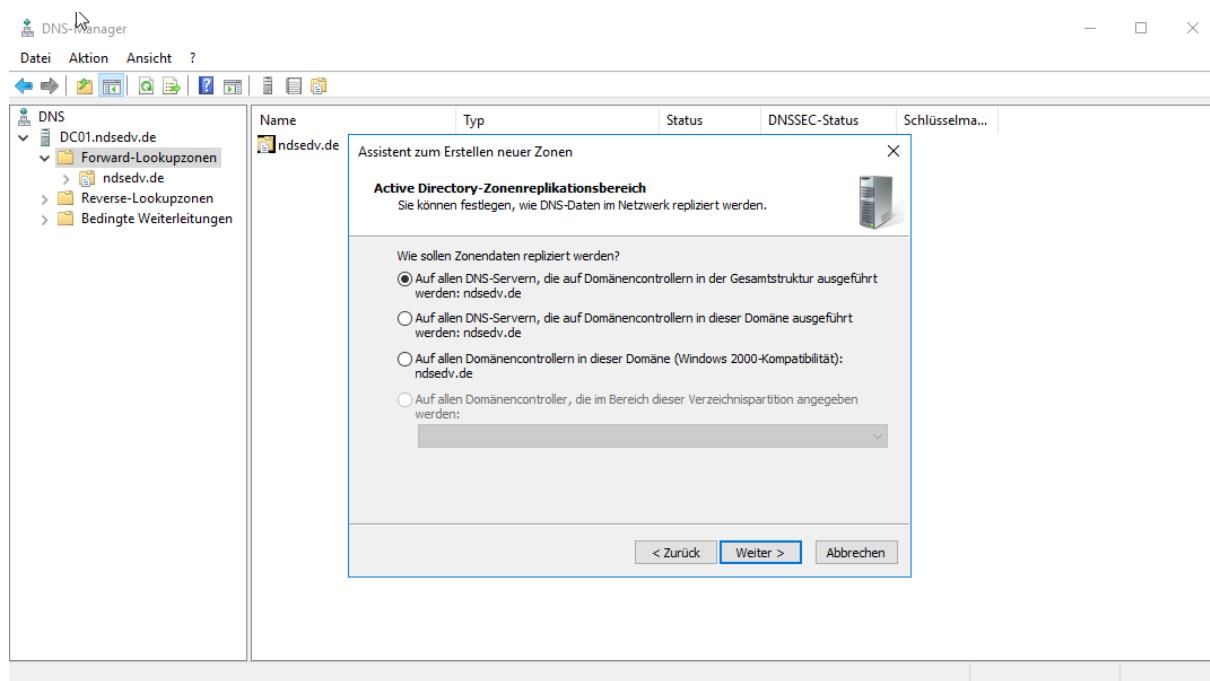
Legen die neue primäre Zone _msdcs.ndsedv.de forestweit an.



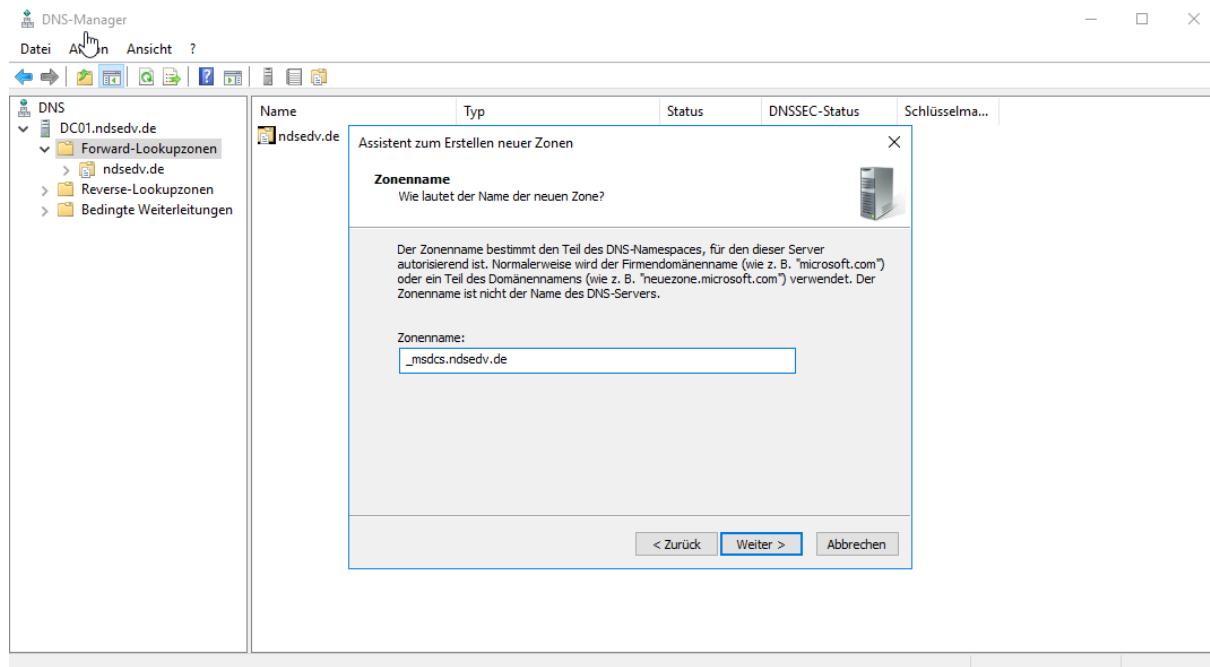


_msdcs Zone gesamtstrukturweit neu anlegen

Soll in der Gesamtstruktur repliziert werden.



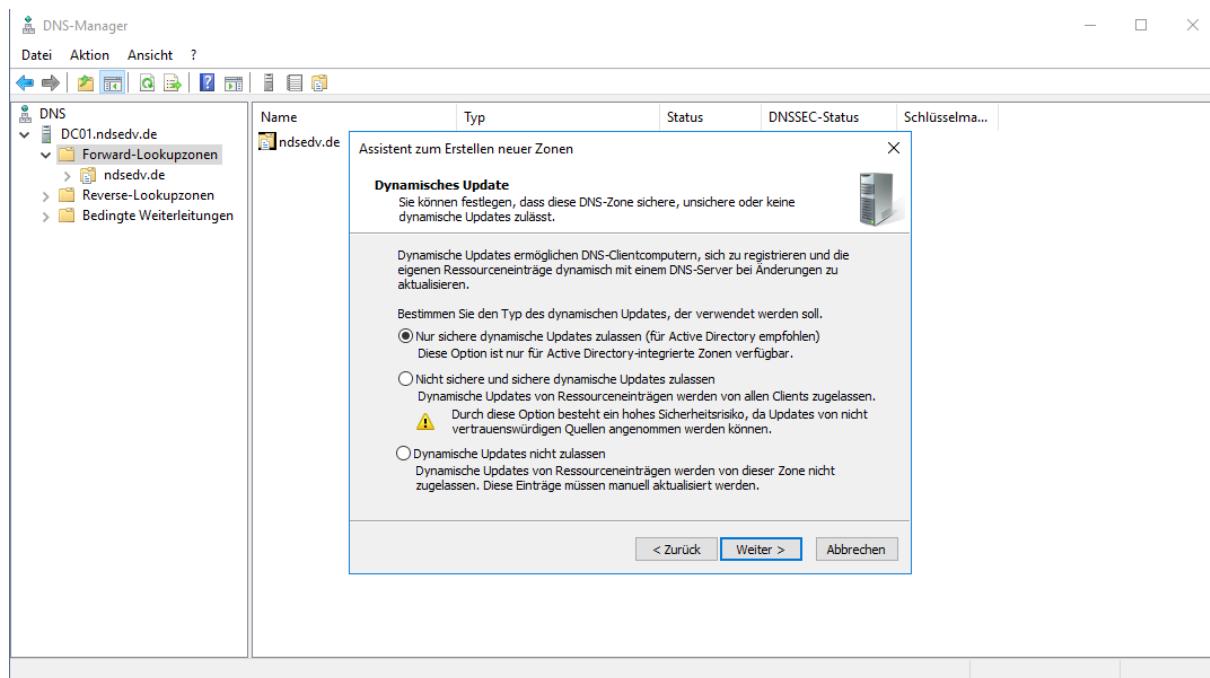
Name der Zone `_msdcs.ndsedv.de`



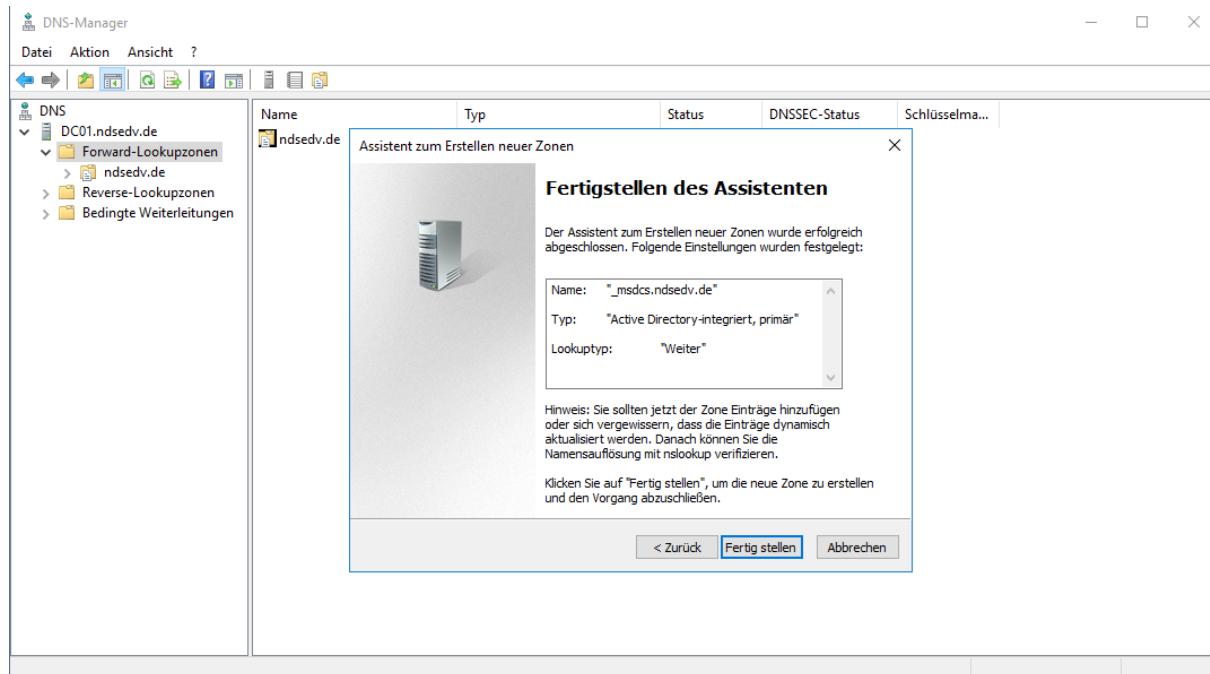


_msdcs Zone gesamtstrukturweit neu anlegen

Aus Gründen der Sicherheit nur sichere dynamische Updates zulassen.



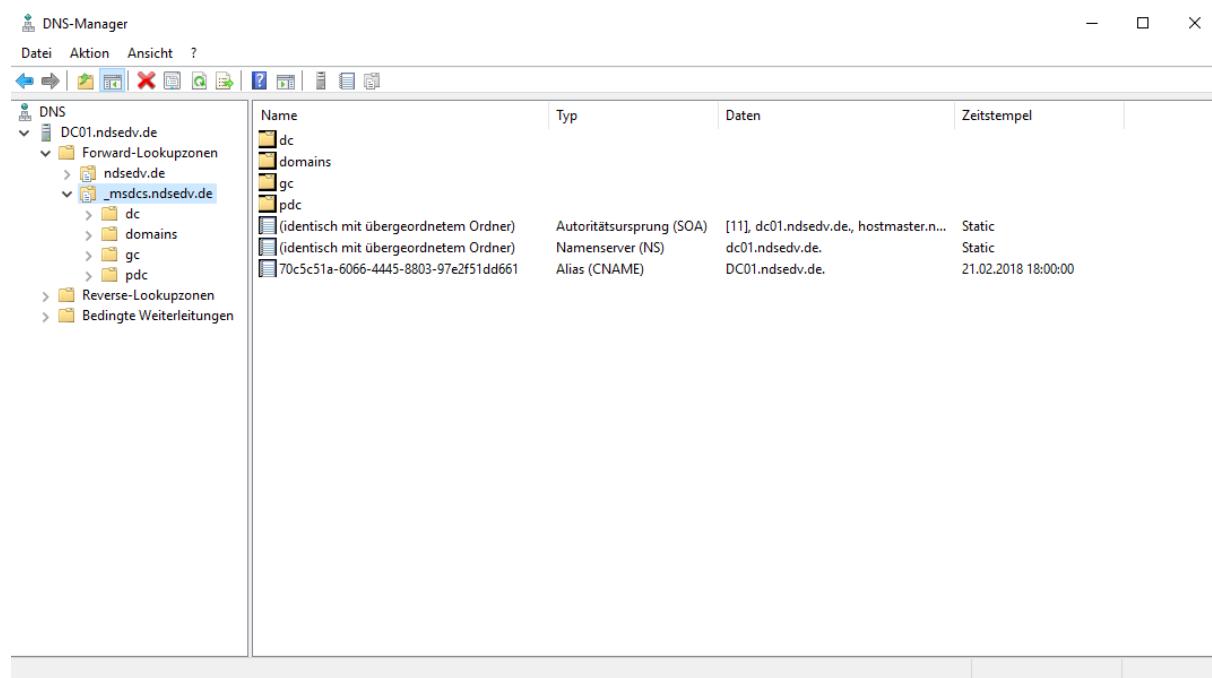
Zusammenfassung





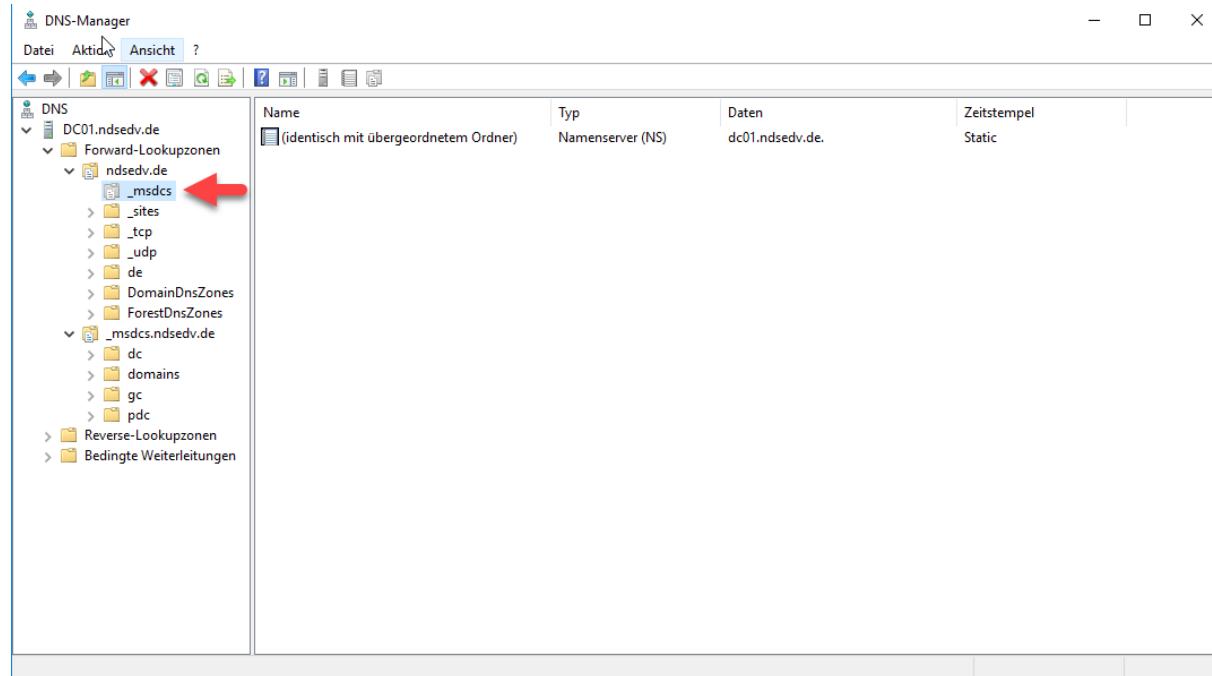
_msdcs Zone gesamtstrukturweit neu anlegen

Die Zone wurde erstellt und der erste (SOA) Eintrag wurde automatisch angelegt.



The screenshot shows the Windows DNS Manager interface. The left pane displays a tree structure of DNS zones under 'DC01.ndsedv.de'. The 'Forward-Lookupzonen' node is expanded, showing sub-zones like 'ndsedv.de', '_msdcs.ndsedv.de', and '_sites'. The '_msdcs.ndsedv.de' node is selected and highlighted with a blue border. The right pane is a table showing DNS records for this zone. The table has columns: 'Name', 'Typ', 'Daten', and 'Zeitstempel'. It contains three entries: an SOA record with 'Name' '(identisch mit übergeordnetem Ordner)', 'Typ' 'Autoritätsursprung (SOA)', 'Daten' '[11], dc01.ndsedv.de, hostmaster.n...', and 'Zeitstempel' 'Static'; an NS record with 'Name' '(identisch mit übergeordnetem Ordner)', 'Typ' 'Namenserver (NS)', 'Daten' 'dc01.ndsedv.de.', and 'Zeitstempel' 'Static'; and a CNAME record with 'Name' '70c5c51a-6066-4445-8803-97e2f51dd661', 'Typ' 'Alias (CNAME)', 'Daten' 'DC01.ndsedv.de.', and 'Zeitstempel' '21.02.2018 18:00:00'.

Die Zone unterhalb der Domäne wurde auch angelegt.



The screenshot shows the Windows DNS Manager interface. The left pane displays a tree structure of DNS zones under 'DC01.ndsedv.de'. The 'Forward-Lookupzonen' node is expanded, showing sub-zones like '_sites', '_tcp', '_udp', 'de', 'DomainDnsZones', 'ForestDnsZones', and '_msdcs.ndsedv.de'. The '_msdcs.ndsedv.de' node is selected and highlighted with a blue border. A red arrow points to this node. The right pane is a table showing DNS records for this zone. The table has columns: 'Name', 'Typ', 'Daten', and 'Zeitstempel'. It contains one entry: an NS record with 'Name' '(identisch mit übergeordnetem Ordner)', 'Typ' 'Namenserver (NS)', 'Daten' 'dc01.ndsedv.de.', and 'Zeitstempel' 'Static'.



_msdcs Zone gesamtstrukturweit neu anlegen

Neustart der Dienste DNSServer und Netlogon.

Services

File Action View Help

Services (Local) Services (Local)

Service Control

Windows is attempting to start the following service on Local Computer...

DNS Server

Close

service is stopped; DNS updates will not occur. If this service is disabled, any services that explicitly depend on it will fail to start.

	Description	Status	Startup Type	Log On As
Association Service	Enables pairing between the system and...	Manual (Trigger Start)	Local System	
Install Service	Enables a computer to recognize and...	Manual (Trigger Start)	Local System	
Management Enrollment Service	Performs Device Enrollment Activities f...	Manual	Local System	
Setup Manager	Enables the detection, download and in...	Manual (Trigger Start)	Local System	
Background Discovery Broker	Enables apps to discover devices with a...	Manual (Trigger Start)	Local System	
Space	Enables you to group shared folders loc...	Automatic	Local System	
Synchronization	Enables you to synchronize folder...	Automatic	Local System	
Ent	Registers and updates IP addresses and...	Automatic	Local System	
Diagnostic Policy Service	The Diagnostic Policy Service enables p...	Running	Automatic (Delayed Start)	
Diagnostic Service Host	The Diagnostic Service Host is used by ...	Manual	Local System	
Diagnostic System Host	The Diagnostic System Host is used by ...	Manual	Local System	
Distributed Link Tracking Client	Maintains links between NTFS files with...	Manual	Local System	
Distributed Transaction Coordinator	Coordinates transactions that span multi...	Running	Automatic (Delayed Start)	
dmwappushsvc	WAP Push Message Routing Service	Manual (Trigger Start)	Local System	
DNS Client	The DNS Client service (dnscache) cach...	Running	Automatic (Trigger Start)	
DNS Server	Enables DNS clients to resolve DNS na...	Running	Automatic (Delayed Start)	
Downloaded Maps Manager	Windows service for application access ...	Manual	Network Service	
DS Role Server	This service hosts the DS Role Server us...	Manual	Local System	
Embedded Mode	The Embedded Mode service enables s...	Manual (Trigger Start)	Local System	
Encrypting File System (EFS)	Provides the core file encryption techn...	Running	Automatic (Trigger Start)	
Enterprise App Management Service	Enables enterprise application manage...	Manual	Local System	
Extensible Authentication Protocol	The Extensible Authentication Protocol ...	Manual	Local System	
File Replication	Synchronizes folders with file servers th...	Disabled	Local System	
Function Discovery Provider Host	The FDHOST service hosts the Function D...	Manual	Local System	
Function Discovery Resource Publication	Publishes this computer and resources ...	Manual	Local System	
Geolocation Service	This service monitors the current locati...	Running	Manual (Trigger Start)	
Group Policy Client	The service is responsible for applying s...	Running	Automatic (Trigger Start)	
Human Interface Device Service	Activates and maintains the use of hot ...	Manual (Trigger Start)	Local System	
HV Host Service	Provides an interface for the Hyper-V h...	Manual (Trigger Start)	Local System	
Hvov-V Data Exchange Service	Provides a mechanism to exchange dat...	Manual (Trigger Start)	Local System	

Extended Standard

Services

File Action View Help

Services (Local) Services (Local)

Service Control

Windows is attempting to start the following service on Local Computer...

Netlogon

Close

and services. If this service is stopped, the computer may not authenticate users and services and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start.

	Description	Status	Startup Type	Log On As
Port Sharing Service	Provides ability to share TCP ports over the net.tcp protocol.	Disabled	Local Service	
Connection Broker	Maintains a secure channel between this computer and the domain controller.	Running	Automatic	
Connections	Brokers connections that allow Windows Store Apps to receive notifications.	Running	Manual (Trigger Start)	
Connectivity Assistant	Manages objects in the Network and Dial-Up Connections folder, in which...	Running	Manual	
List Service	Provides DirectAccess status notification for UI components.	Manual (Trigger Start)	Local System	
Location Awareness	Identifies the networks to which the computer has connected, collects and...	Running	Manual	
Setup Service	Collects and stores configuration information for the network and notifies...	Automatic	Network Service	
Network Store Interface Service	The Network Setup Service manages the installation of network drivers an...	Manual (Trigger Start)	Local System	
NSClient++ (x64)	This service delivers network notifications (e.g. interface addition/deleti...	Running	Automatic	
OfficeScan Common Client Solution	Monitoring agent for nagios (and others) used to respond to status queries.	Running	Automatic	
OfficeScan NT Listener	Manages advanced solutions and features on Trend Micro OfficeScan age...	Manual	Local System	
OfficeScan NT RealTime Scan	Receives commands and notifications from the OfficeScan server and facili...	Running	Automatic	
Offline Files	Performs Real-time, Scheduled, and Manual scan on Trend Micro OfficeSc...	Running	Automatic	
Optimize drives	The Offline Files service performs maintenance activities on the Offline Fil...	Disabled	Local System	
Performance Counter DLL Host	Helps the computer run more efficiently by optimizing files on storage dri...	Manual	Local System	
Performance Logs & Alerts	Enables remote users and 64-bit processes to query performance counters ...	Manual	Local Service	
Phone Service	Performance Logs and Alerts Collects performance data from local or rem...	Manual	Local Service	
Plug and Play	Manages the telephony state on the device.	Manual (Trigger Start)	Local Service	
Portable Device Enumerator Service	Enables a computer to recognize and adapt to hardware changes with littl...	Running	Manual	
Power	Enforces group policy for removable mass-storage devices. Enables applic...	Manual (Trigger Start)	Local System	
Print Spooler	This service spools print jobs and handles interaction with the printer. If y...	Running	Automatic	
Printer Extensions and Notifications	This service opens custom printer dialog boxes and handles notifications f...	Manual	Local System	
Problem Reports and Solutions Con...	This service provides support for viewing, sending and deletion of system...	Manual	Local System	
Program Compatibility Assistant Se...	This service provides support for the Program Compatibility Assistant (PC...	Running	Automatic	
Quality Windows Audio Video Experi...	Quality Windows Audio Video Experience (qWave) is a networking platfor...	Manual	Local Service	
Radio Management Service	Radio Management and Airplane Mode Service	Manual	Local Service	
Remote Access Auto Connection M...	Creates a connection to a remote network whenever a program references...	Disabled	Local System	
Remote Access Connection Manager	Manages dial-up and virtual private network (VPN) connections from this ...	Disabled	Local System	
Remote Desktop Configuration	Remote Desktop Configuration service (RDCS) is responsible for all Remot...	Running	Manual	
Remote Desktop Services	Allows users to connect interactively to a remote computer. Remote Deskt...	Running	Manual	
Remote Desktop Services UserMod...	Allows the redirection of Printers/Drives/Ports for RDP connections	Running	Manual	
Remote Procedure Call (RPC)	The RPCSS service is the Service Control Manager for COM and DCOM calls.	Running	Automatic	

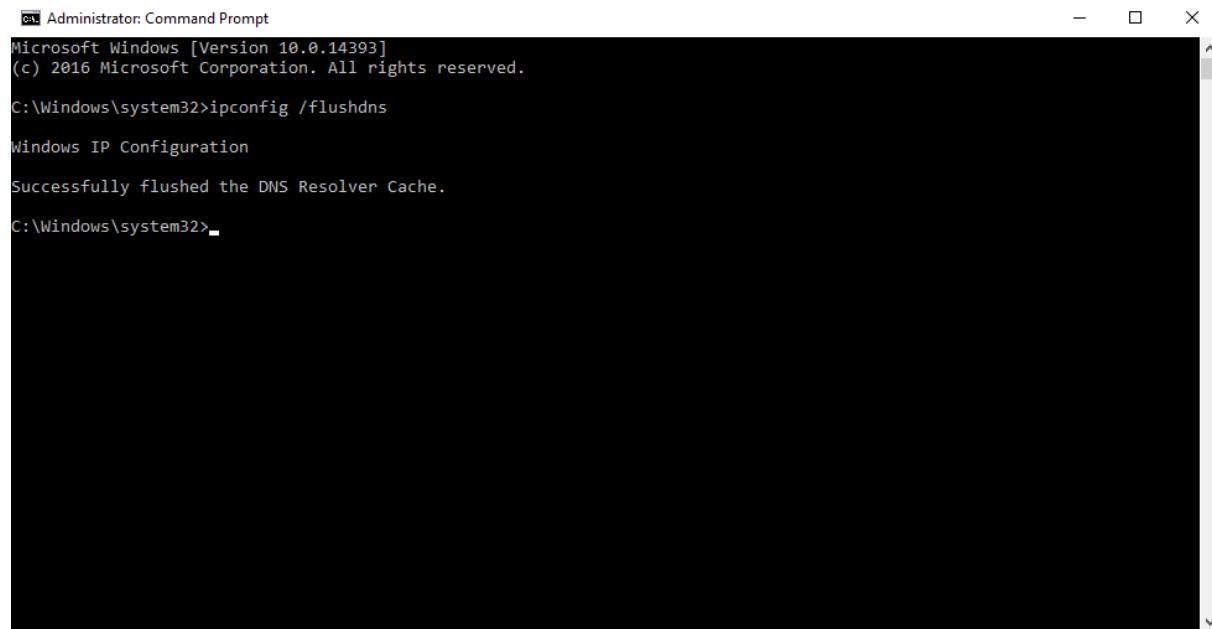
Extended Standard



_msdcs Zone gesamtstrukturweit neu anlegen

Löschen des lokalen Cache auf dem DC.

Ipconfig /flushdns



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

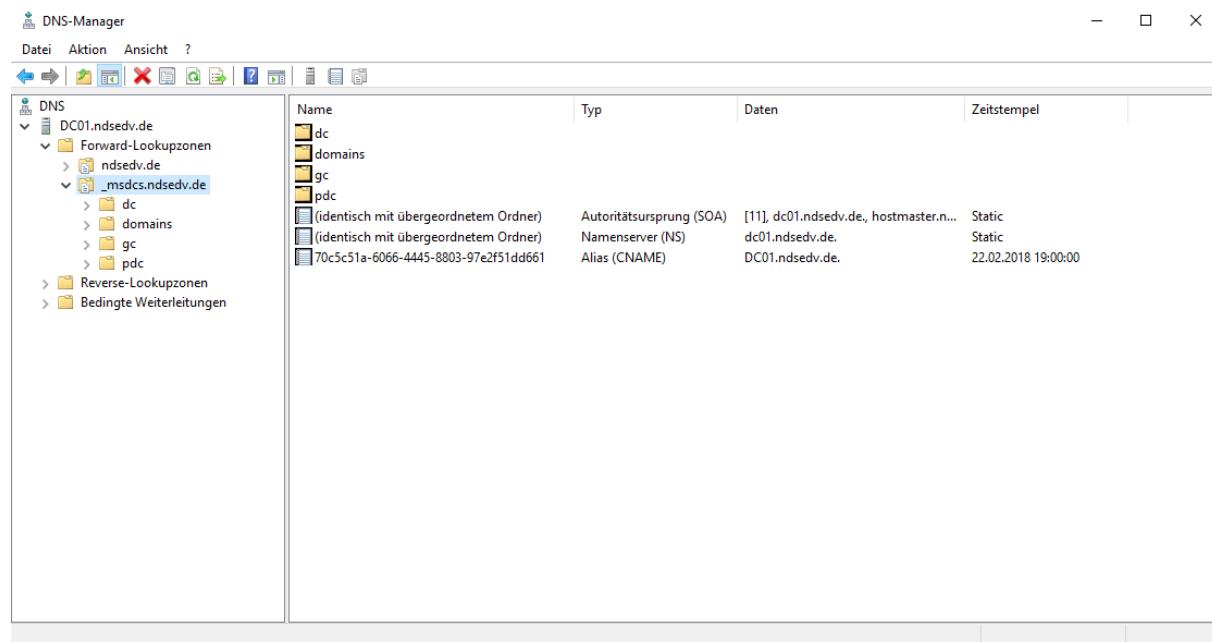
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>
```

Die zu erwartenden Nameserver und Einträge sind nun vorhanden.



The screenshot shows the Windows DNS-Manager interface. The left pane displays a tree structure of DNS zones under 'DC01.ndsedv.de'. The 'Forward-Lookupzonen' section contains 'ndsedv.de' and '_msdcs.ndsedv.de'. The '_msdcs.ndsedv.de' node is expanded, showing subfolders 'dc', 'domains', 'gc', and 'pdc'. The right pane is a table listing DNS records for the '_msdcs' zone:

Name	Typ	Daten	Zeitstempel
(identisch mit übergeordnetem Ordner)	Autoritätsursprung (SOA)	[11], dc01.ndsedv.de, hostmaster.n...	Static
(identisch mit übergeordnetem Ordner)	Namenserver (NS)	dc01.ndsedv.de.	Static
70c5c51a-6066-4445-8803-97e2f51dd661	Alias (CNAME)	DC01.ndsedv.de.	22.02.2018 19:00:00



_msdcs Zone gesamtstrukturweit neu anlegen

Diese Prozedur ist auf allen DC durchzuführen:

Forward und Reverse Eintrag löschen und die beiden Dienste durchstarten, anschließend neu registrieren und den lokalen Cache löschen.

```
Administrator: Eingabeaufforderung

C:\Windows\system32>net stop dns
DNS-Server wird beendet.
DNS-Server wurde erfolgreich beendet.

C:\Windows\system32>net stop netlogon
Anmeldedienst wird beendet.
Anmeldedienst wurde erfolgreich beendet.

C:\Windows\system32>net start dns
DNS-Server wird gestartet.
DNS-Server wurde erfolgreich gestartet.

C:\Windows\system32>net start netlogon
Anmeldedienst wird gestartet..
Anmeldedienst wurde erfolgreich gestartet.

C:\Windows\system32>ipconfig /registerdns

Windows-IP-Konfiguration

Die Registrierung der DNS-Ressourceneinträge für alle Adapter dieses Computer wurde initialisiert. Fehler werden in der Ereignisanzeige in 15 Minuten aufgeführt.

C:\Windows\system32>
```

Zur Sicherheit starten wir einen manuellen Sync nach dem wir auf allen DCs die Dienste durchgestartet haben.

```
Administrator: Command Prompt

C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>repadmin /syncall
CALLBACK MESSAGE: The following replication is in progress:
  From: 5504a722-8fa7-49ef-ad98-c26d370ce000._msdcs.easycash.de
  To : 606bf154-977d-43c7-846a-f2ca53414323._msdcs.easycash.de
CALLBACK MESSAGE: The following replication completed successfully:
  From: 5504a722-8fa7-49ef-ad98-c26d370ce000._msdcs.easycash.de
  To : 606bf154-977d-43c7-846a-f2ca53414323._msdcs.easycash.de
CALLBACK MESSAGE: The following replication is in progress:
  From: 606bf154-977d-43c7-846a-f2ca53414323._msdcs.easycash.de
  To : 1effb37a-885e-47bb-8a99-3223fb2666e1._msdcs.easycash.de
CALLBACK MESSAGE: The following replication completed successfully:
  From: 606bf154-977d-43c7-846a-f2ca53414323._msdcs.easycash.de
  To : 1effb37a-885e-47bb-8a99-3223fb2666e1._msdcs.easycash.de
CALLBACK MESSAGE: The following replication is in progress:
  From: 3105a287-4685-479d-a6e0-1f79a57cc221._msdcs.easycash.de
  To : 1effb37a-885e-47bb-8a99-3223fb2666e1._msdcs.easycash.de
CALLBACK MESSAGE: The following replication completed successfully:
  From: 3105a287-4685-479d-a6e0-1f79a57cc221._msdcs.easycash.de
  To : 1effb37a-885e-47bb-8a99-3223fb2666e1._msdcs.easycash.de
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

C:\Windows\system32>
```

<https://support.microsoft.com/en-us/help/817470/how-to-reconfigure-an-msdcs-subdomain-to-a-forest-wide-dns-application>



_msdcs Zone gesamtstrukturweit neu anlegen

BPA TEST vorher:

Local Server - BPA Results Detail View

3 BPA results

Severity levels: Error Categories: All
Servers: All

Server Name	Severity	Title	Category
A-SSB-ADS1	Error	DNS: DNS servers on Ethernet0 should include the loopback address, but not as the first entry.	Configuration
A-SSB-ADS1	Error	DNS: At least one name server in the list of root hints must respond to queries for the root zone.	Configuration
A-SSB-ADS1	Error	DNS: Zone _msdcs. [REDACTED].de is an Active Directory integrated DNS Zone and must be available.	Configuration

Go To Local Server OK Cancel

BPA TEST nachher: **bestanden**

Local Server - BPA Results Detail View

2 BPA results

Severity levels: Error Categories: All
Servers: All

Server Name	Severity	Title	Category
A-SSB-ADS1	Error	DNS: DNS servers on Ethernet0 should include the loopback address, but not as the first entry.	Configuration
A-SSB-ADS1	Error	DNS: At least one name server in the list of root hints must respond to queries for the root zone.	Configuration

Go To Local Server OK Cancel