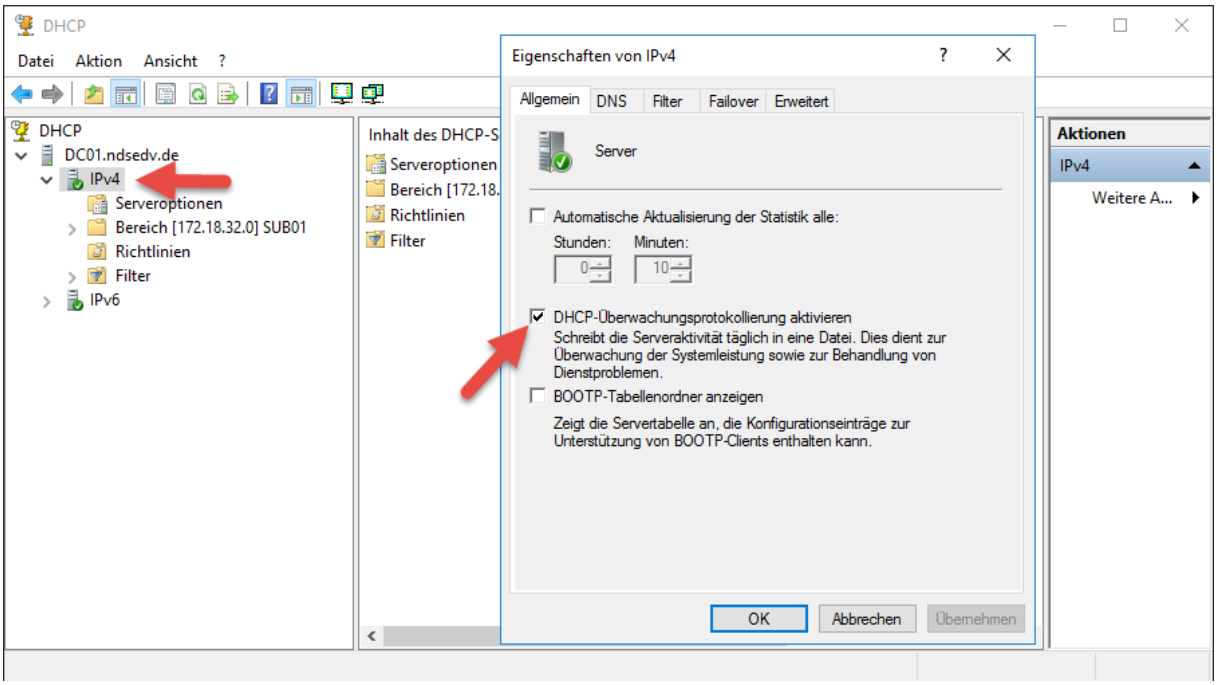
DHCP Auditing und DHCP Service stoppt

DHCP steht für Dynamic Host Configuration Protocol. Der DHCP Dienst gibt in einem Netzwerk automatisch IP-Adressen an die Arbeitsstationen aus. Der zentrale Zweig von DHCP ist die Integration in DNS (Domain Name System). Das Ziel der Integration ist die automatische Registrierung von Hostnamen und IP-Adressen bei DNS-Servern durch den DHCP-Server.

Der Client sendet ein DHCP-Discover (Broadcast) ins Netzwerk und erwartet von einem vorhandenen DHCP-Server ein DHCP-Offer (eine IP Adresse angeboten). Der Client nimmt die ihm angebotene IP Adresse (DHCP-Offer) an und sendet dem DHCP-Server ein DHCP-Request (ich nehme dein Angebot an). Der DHCP-Server bestätigt mit einem DHCP-Acknowledge (damit sind wir im Geschäft). Wird kein DHCP-Server erreicht, bekommt der Client über APIPA (Automatic Private IP Adressing) eine vorläufige IP aus dem Bereich 169.254.0.1 – 255.254.

Zur Nachverfolgung solcher Aktionen ist es wichtig, das die Auditing-Funktion aktiviert wird.



Auditing aktivieren maximale Logging Größe und Pfad bestimmen:

```
Set-DhcpServerAuditLog -ComputerName "DC01.ndsedv.de" -Enable $True -Path "C:\Logs\DHCP\Auditing\dhcpauditlog\" -MaxMBFileSize 100
```

Per Registry nur das Auditing aktivieren

```
reg add HKLM\System\CurrentControlSet\Services\DhcpServer\Parameters /v ActivityLogFlag /t REG_DWORD /d 1
```

Maximale Logging Größe aller zu erstellenden Audit Logs anpassen:

```
Set-DhcpServerAuditLog -MaxMBFileSize 250
Set-DhcpServerAuditLog -MaxMBFileSize 4096
```

Dateipfade für die Logdateien anpassen:

```
netsh dhcp server set databasepath D:\Logs\DHCP
netsh dhcp server set auditlog D:\Logs\DHCP\Auditing\dhcpauditlog
```

Erstellt von Jörn Walter **25.02.2019**

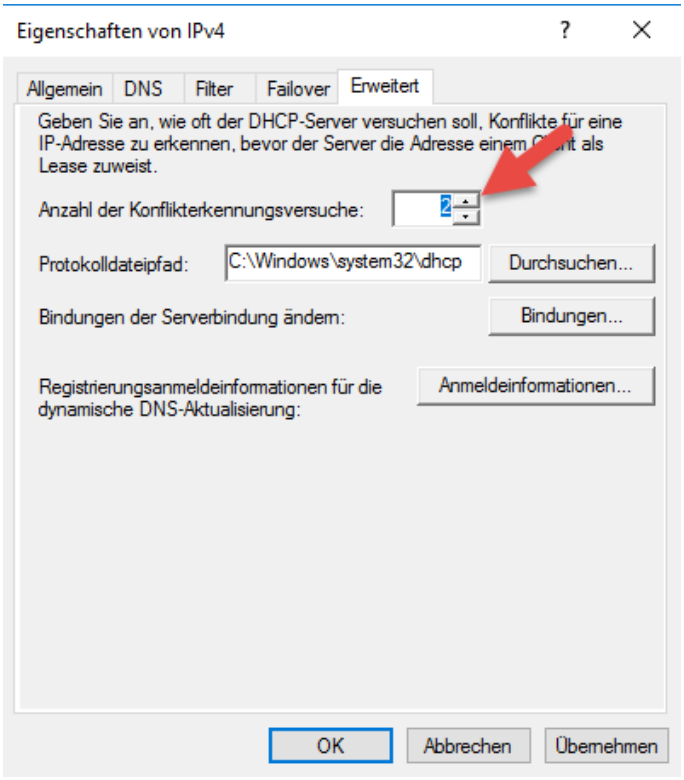
DHCP Auditing und DHCP Service stoppt

Hinweis:

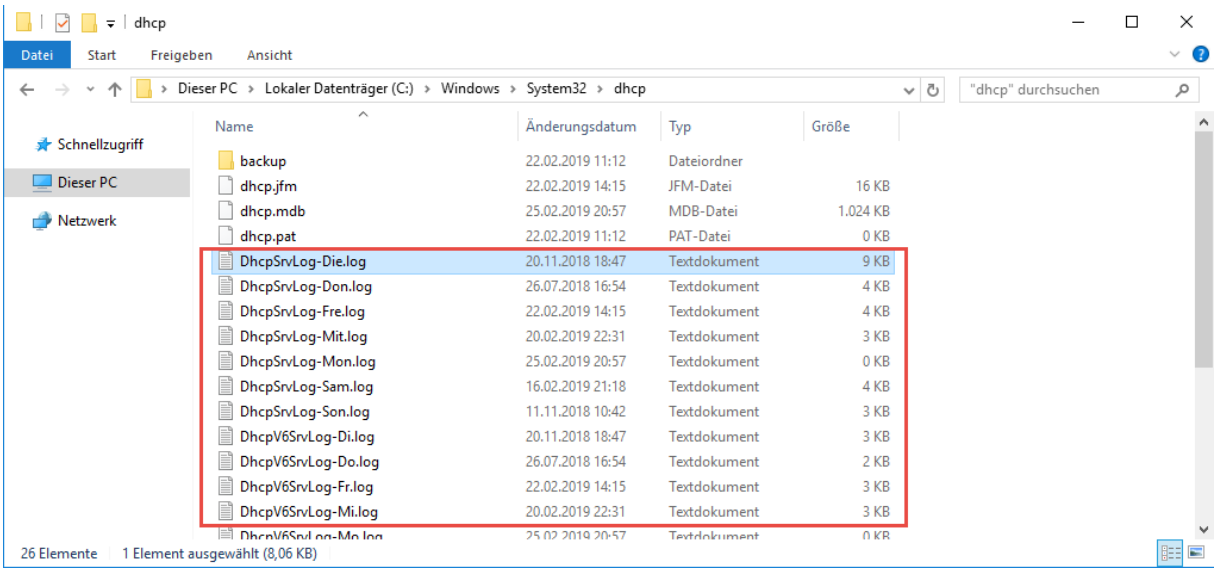
Bei dem Parameter MaxMBFileSize handelt es sich um die addierte Größe aller erstellen Log-Dateien. Wenn die maximale Größe aller addierten Log-Dateien den MaxMBFileSize übersteigt, wird das Logging eingestellt und es werden keine IP-Adressen mehr ausgegeben.

DHCP Konflikterkennungsversuche aktivieren:

Wenn die Erkennung aktiviert ist, startet der DHCP Server einen Ping-Prozess, um die verfügbaren IP-Bereiche zu ermitteln. Erst danach wird der DHCP Lease einem Client angeboten. Der Wert sollte auf 2 stehen um die Netzwerklast nicht zu erhöhen.



Sobald das Auditing aktiviert ist, wird für jeden Tag eine neue Log-Datei angelegt:



DHCP Auditing und DHCP Service stoppt

Ereignis-ID Bedeutung

00	Das Protokoll wurde gestartet.
01	Das Protokoll wurde beendet.
02	Das Protokoll wurde aufgrund von unzureichendem Speicherplatz temporär angehalten.
10	Für einen Client wurde eine neue IP-Adresse geleast.
11	Eine Lease wurde von einem Client erneuert.
12	Eine Lease wurde von einem Client freigegeben.
13	Es wurde ermittelt, dass eine IP-Adresse im Netzwerk verwendet wird.
14	Eine Leaseanforderung konnte nicht erfüllt werden, da der Adresspool des Bereichs erschöpft war.
15	Eine Lease wurde verweigert.
16	Eine Lease wurde gelöscht.
17	Eine Lease war abgelaufen, und die DNS-Einträge für eine abgelaufene Lease wurden nicht gelöscht.
18	Eine Lease war abgelaufen, und die DNS-Einträge wurden gelöscht.
20	Eine BOOTP-Adresse wurde einem Client geleast.
21	Eine dynamische BOOTP-Adresse wurde einem Client geleast.
22	Eine BOOTP-Anforderung konnte nicht erfüllt werden, da der Adresspool für BOOTP des Bereichs erschöpft war.
23	Eine BOOTP-IP-Adresse wurde gelöscht, nachdem sichergestellt wurde, dass sie nicht verwendet wird.
24	Der Bereinigungsvorgang für die IP-Adresse wurde gestartet.
25	Statistik der IP-Adressenbereinigung.
30	DNS-Updateanforderung an den benannten DNS-Server.
31	Fehler beim DNS-Update.
32	Das DNS-Update war erfolgreich.
33	Das Paket wurde aufgrund der NAP-Richtlinie verworfen.
34	Fehler bei der DNS-Updateanforderung: Die maximale Anzahl von DNS-Updateanforderungen in der Warteschlange wurde überschritten.
35	Fehler bei der DNS-Updateanforderung.
36	Das Paket wurde verworfen, da sich der Server in der Failoverstandbyrolle befindet oder der Hash der Client-ID abweicht.
50+	Codes über 50 werden für Informationen über die Erkennung nicht autorisierter Server verwendet.

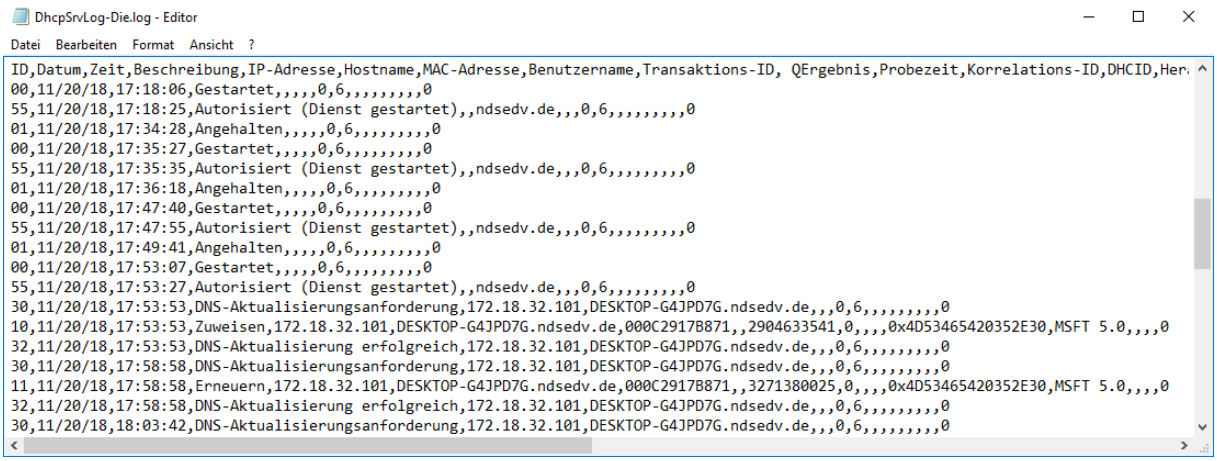
Erstellt von Jörn Walter **25.02.2019**

DHCP Auditing und DHCP Service stoppt

Jeder Eintrag in dem Log steht in einer separaten Zeile:

Die Einträge enthalten Informationen zu

- ID = Event Code
- Date = Datum des Log Eintrags
- Time = Zeit des Log Eintrags
- Description = Beschreibung des Events
- IP Address = IP Adresse des DHCP Clients
- Host Name = Name des DHCP Servers
- Mac Address = MAC Adresse des Netzwerkadapters



Nach einer Woche werden die gespeicherten Logdateien wieder überschrieben.

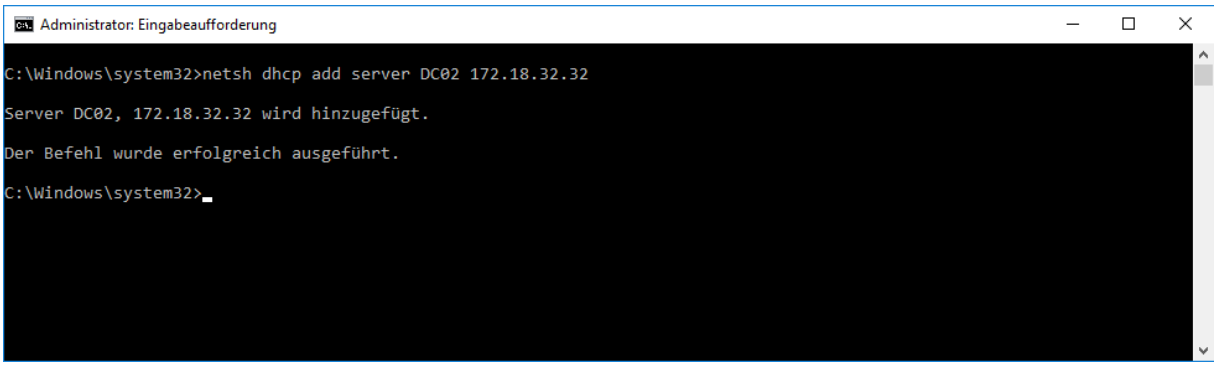
Abfragen wie viele DHCP Servers es gibt:

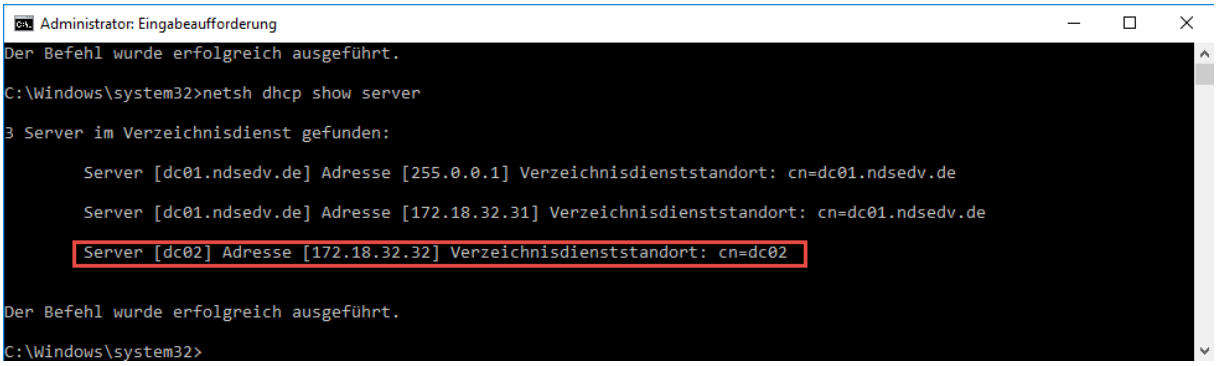
netsh dhcp show server

DHCP Auditing und DHCP Service stoppt

DHCP Server autorisierend hinzufügen:

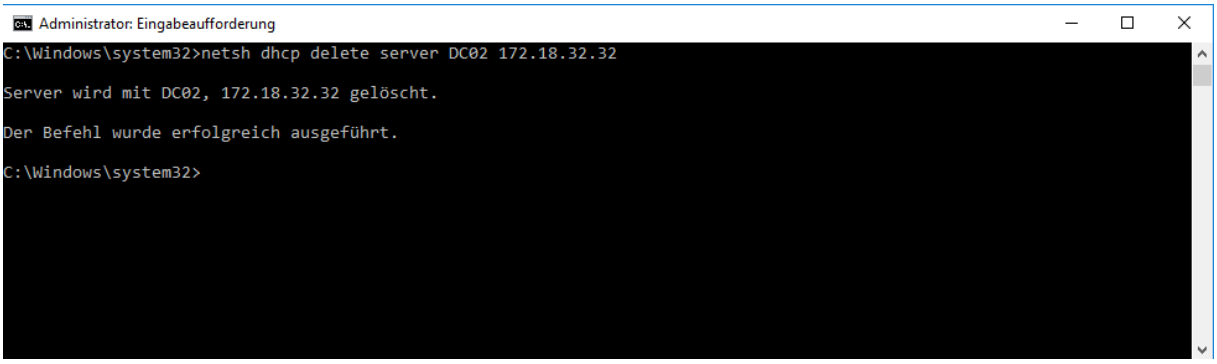
netsh dhcp add server DC02 172.18.32.32





DHCP Server Autorisierung aufheben:

netsh dhcp delete server DC02 172.18.32.32

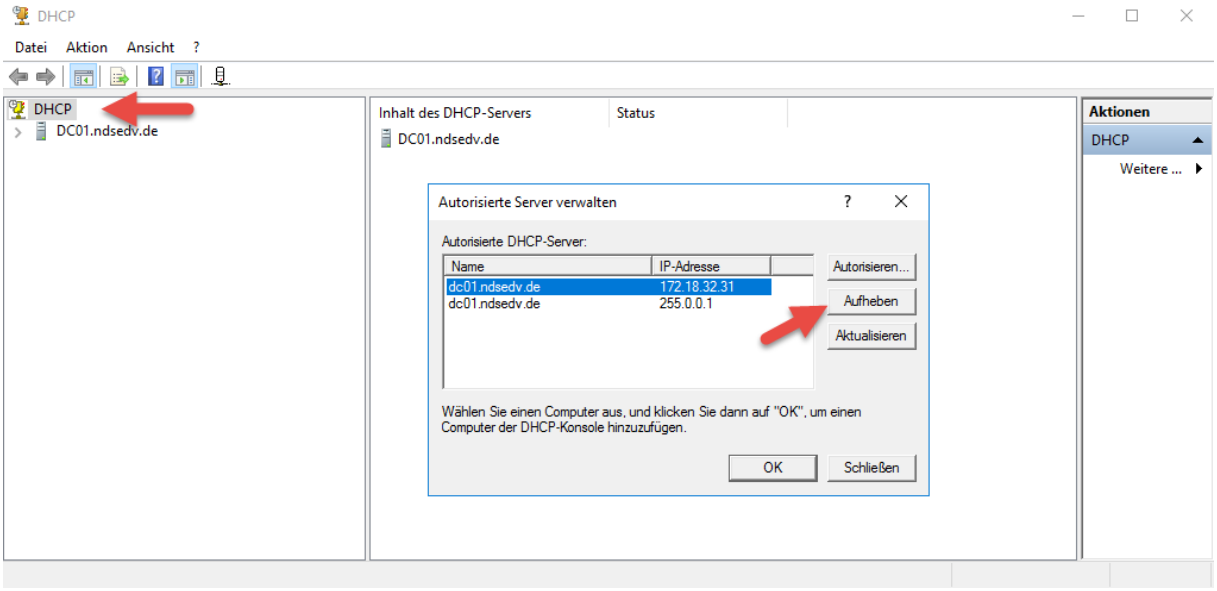


Hinweis:

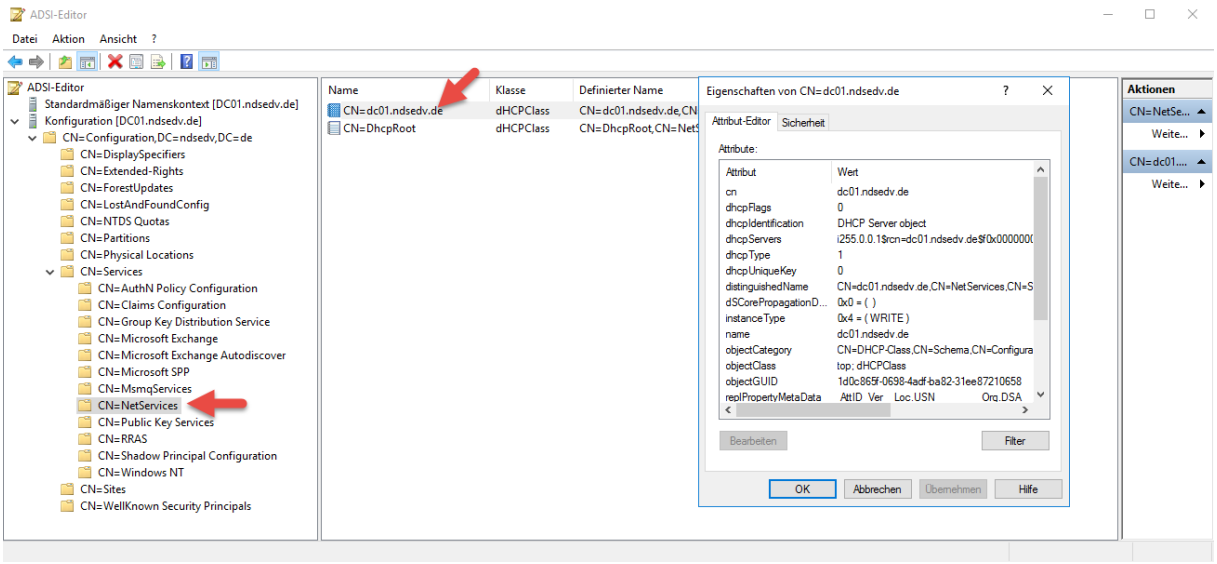
Sollte die Aufhebung der Autorisierung über die GUI oder CMD nicht zum Erfolg führen, so können die alten DHCP-Server über die MMC ADSIEdit gelöscht werden.

DHCP Auditing und DHCP Service stoppt

Aufhebung der Autorisierung über die GUI



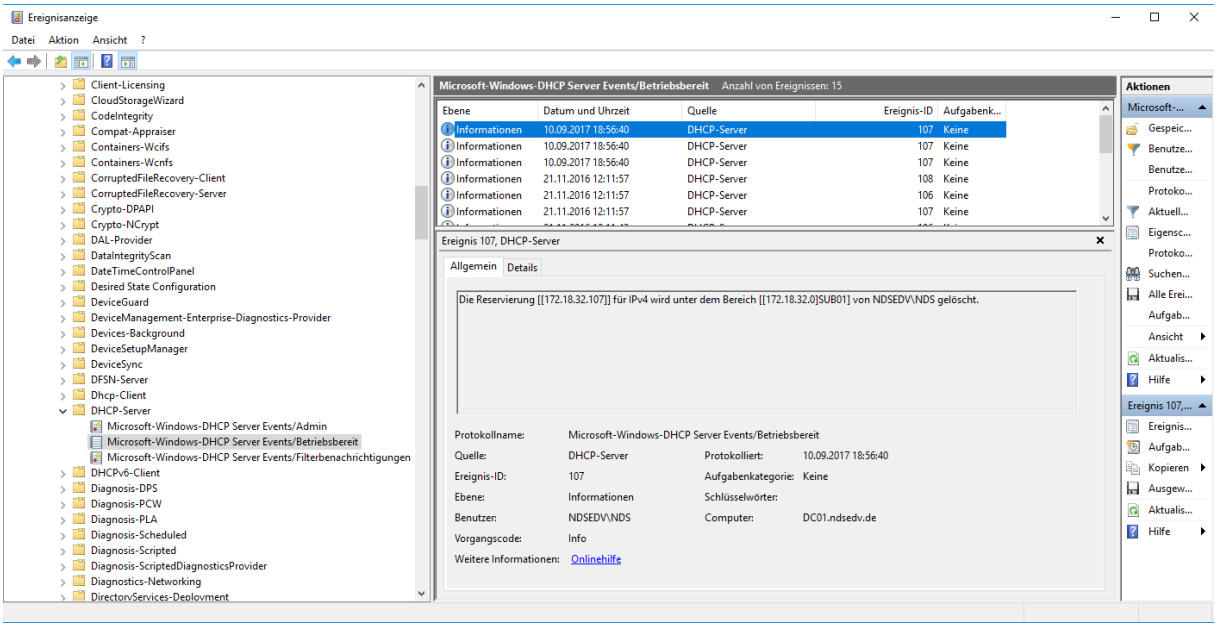
DHCP Server - Ansicht über ADSIEdit:



Erstellt von Jörn Walter **25.02.2019**

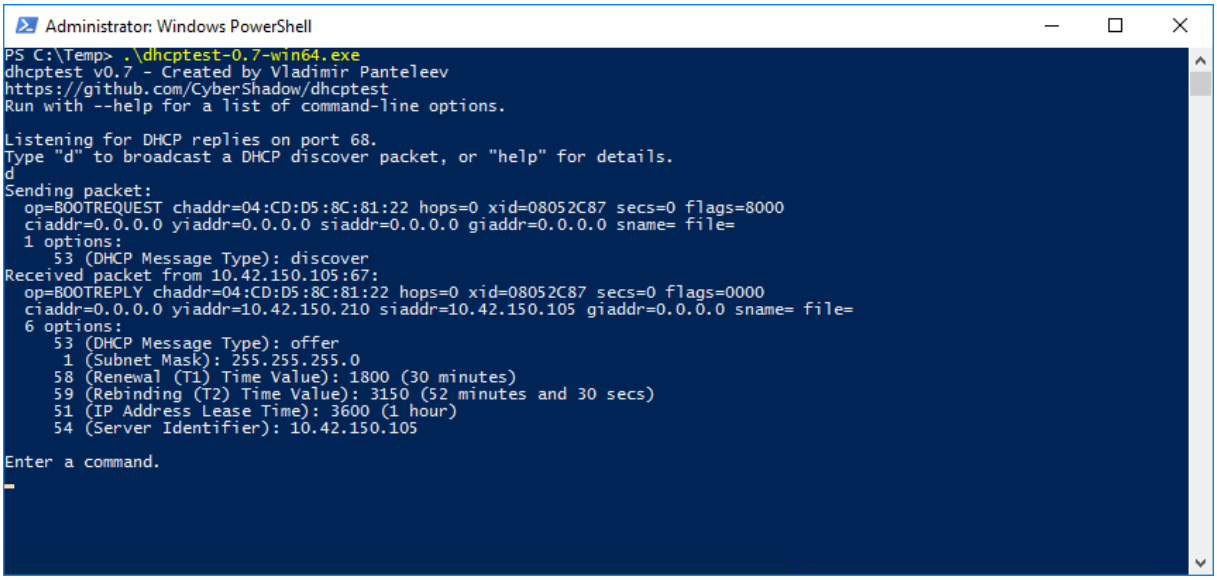
DHCP Auditing und DHCP Service stoppt

Eingesetzte Softwareprodukte wie AD Audit von Manage Engine oder Arcsight, benötigen diese Logs für das Compliance Management.



DHCP Test:

https://files.thecybershadow.net/dhcptest/
https://github.com/CyberShadow/dhcptest



Weitere Ereignis-ID Bedeutungen ab ID 50:

50 - The DHCP server could not locate the necessary domain.

51 - Authorization was successful.

52 - The server was recently upgraded to Windows Server 2003 Standard Edition. During the upgrade process, the unauthorized DHCP server detection mechanism, which is used to determine whether or not the DHCP server has been authorized in the active directory, was disabled.

Erstellt von Jörn Walter **25.02.2019**

53 - The Active Directory was inaccessible at the time that the DHCP services started. Because of this, cached information was used to authorize the DHCP services to start.

54 - This is an authorization failure code. When this event occurs, it is because the DHCP server does not authorized within the active directory. An event code and 54 should be followed by an event ID showing that the DHCP services have stopped.

55 - The DHCP services were authorized to start.

56 - Event number 56 was the event that showed up in our sample log file. This event indicates that the DHCP service was not authorized to start, and was consequently shut down. As you probably know, you must authorize a DHCP server in active directory prior to starting the DHCP services.

57 - Another DHCP server already exist within the specified domain.

58 - The DHCP server was unable to locate the necessary domain.

59 - A network connectivity issue prevent the server for determining whether or not it has been authorized.

60 - This error code needs a bit of explaining. The event ID means that no domain controller is Directory Service enabled. This event ID this only encountered in mixed mode environments in which Windows NT domain controllers are present. Because a DHCP server can only be authorized through the Active Directory, the DHCP server must be able to communicate with the Active Directory in order to determine whether it has been authorized or not. Therefore, if the DHCP server is only able to communicate with Windows NT based domain controllers, the log file will reflect an event ID of 60.

61 - This event ID means that another DHCP server that belongs to the same domain was found on the network. This event ID is different from number 57 in that the detected DHCP server does not necessarily have to be authorized. For example, the DHCP services might be running on an old Windows NT server.

62 - Event ID number 62 means that another DHCP server was detected on the network. The difference between event ID number 62 and event ID numbers 61 and 57 is that event ID number 62 is not domain specific. In fact, the DHCP server that is detected does not even have to be a Windows server. This is simply a generic event ID that is produced anytime another DHCP server is detected.

63 - Event ID number 63 is produced when the DHCP server is having trouble with the rogue detection mechanism. This event is generated when the rogue detection mechanism is restarted. Restarting the rogue detection mechanism implies that the server is going to try one more time to determine whether or not it is authorized.

64 - This event ID indicates that there are no DHCP enabled network interfaces. What this means is that none of the server's network interfaces are configured in a way that is acceptable to the DHCP services. Typically this means one of three things. One possibility is that there may not be in network cable plugged into the network adapter in question. A second possibility is that all of the DHCP server's network interfaces might be configured to use dynamic IP addresses. A DHCP server requires at least one static IP address. Finally, the third possibility is that all of the network adapters bound to static IP addresses have been disabled.