Active Directory Health-Check

Was gehört alles zu einem Health Check dazu und was kann mit welchen Hilfsmitteln geprüft werden. Ein Health Check sollte folgende Punkte umfassen:

AD Health Check

- Konnektivität
- DNS
- Replikation
- Performance
- Events

Womit können wir prüfen und was steht uns dabei zur Auswahl?

- Server Manager
  - Dashboard
  - Events
  - Services
  - Best Practice Analyzer
  - Performance
- Diagnose Tools
  - -Performance Monitor
  - -DCdiag
  - -Repadmin
- EventLog
  - DFS-Replikation
  - Verzeichnisdienst
  - DNS-Server

Was kann ich mit dem Server Manager erledigen?

- Dashboard
  - Multiple Server Verwaltung
  - Server Gruppen
  - Health Indikatoren
  - Export/Import
- Events
  - Ansicht
  - Filter
- Services
  - Ansicht
  - Filter
- Best Practice Analyzer
  - Probleme ermitteln
  - Lösungen
- Performance
  - Leistungswarnungen
  - Speicher
  - CPU

Was kann ich mit dem Performance Monitor als Diagnose Tool erledigen?

- Echtzeit Überwachung
- Datensammlersätze
  - Leistungsindikatoren
  - Ereignisablaufverfolgung
  - Systemkonfigurationsinformationen & Bericht

Active Directory Health-Check

- Warnungen
- Berichte
- Zeitplan: gesteuertes sammeln von Daten

Was können wir mit DCdiag als Diagnose Tool prüfen?

Hier nur die wichtigsten Primärtests

- Connectivity (Anfangstest)
  - Wird der DC im DNS aufgelöst?
  - Antwortet der DC auf ICMP Pings?
  - Steht die LDAP Konnektivität
  - Funktioniert das Binding auf LDAP und RPC
- Advertising
  - Prüft die veröffentlichten DS_Flags
    - DCs
    - LDAP Server
    - Beschreibbare oder nur lesende DCs
    - KDC
    - Zeitserver
    - Globaler Katalog
- FrsEvent
  - Nicht mehr nötig, da DFSR übernommen hat
- DFSREvent
  - Prüfung der letzten 24 Stunden Events
- SysVolCheck
  - Registry Wert namens SysvolReady wird geprüft, soll = 1 sein
- KCCEvent
  - Prüft Directory Services im 15 Minuten Intervall
- KnowsOfRoleHolders
  - Prüft ob die DCs wissen wer welche FSMO Rolle hält
- MachineAccount
  - Prüft das Computer Konto des DCs
- NCSecDesc
  - Prüft die Berechtigungen aller Naming Contexts (Schema, Konfiguration etc.) um sicherzustellen das die Replikation zwischen den DCs funktioniert
- NetLogons
  - Prüft ob SysVol und Netlogon erreichbar sind und gelesen werden können
- ObjectReplicated
  - Prüft ob bestimmte Objekte repliziert wurden
- Replications
  - Prüft ob die Replikation aktiv ist und ob die letzte (12 Stunden) auch erfolgreich war
- RidManager
  - Prüft die RID Master Rolle
- Services
  - Prüft ob alle notwendigen Services für das Active Directory laufen
    - RPCSS
    - EventSystem
    - DNSCache
    - NTFRS
    - ISMServ

        - KDC
        - SAMSS
        - Server
        - Workstation
        - W32Time
        - Netlogon
        - NTDS
        - DFSR
- SystemLog
    - Prüft die Einträge der letzten 60 Minuten und gibt Fehler und Warnungen aus
- VerifyReferences
    - Prüft die Computer Referenzen (Attribute wie Site,DFSR usw.)

Was können wir mit Repadmin als Diagnose Tool prüfen?

Wichtige Schalterfunktionen sind:

- replsummary
    - Erzeugt eine kurze und schnelle Zusammenfassung über den Replikationsstatus unserer DCs
- showrepl
    - Zeigt an welche Objekte repliziert wurden
- queue
    - Zeigt die Länge der Warteschlange an
- syncall
    - Startet den Replikationsvorgang erneut
- replicate
    - Startet den Replikationsvorgang erneut

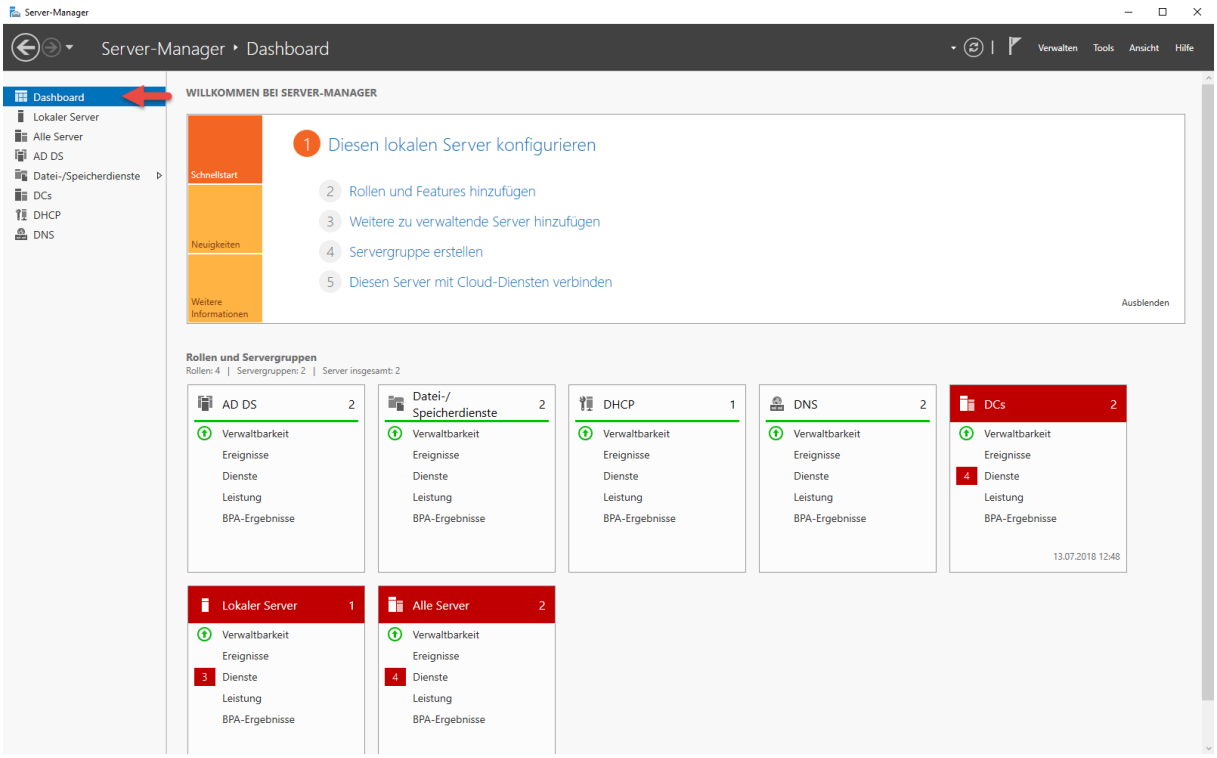
Was sollte im Event Log geprüft werden?

Um sicher zu stellen das alles reibungslos funktioniert sollten man sich gelegentlich auch mal die Event IDs ansehen:

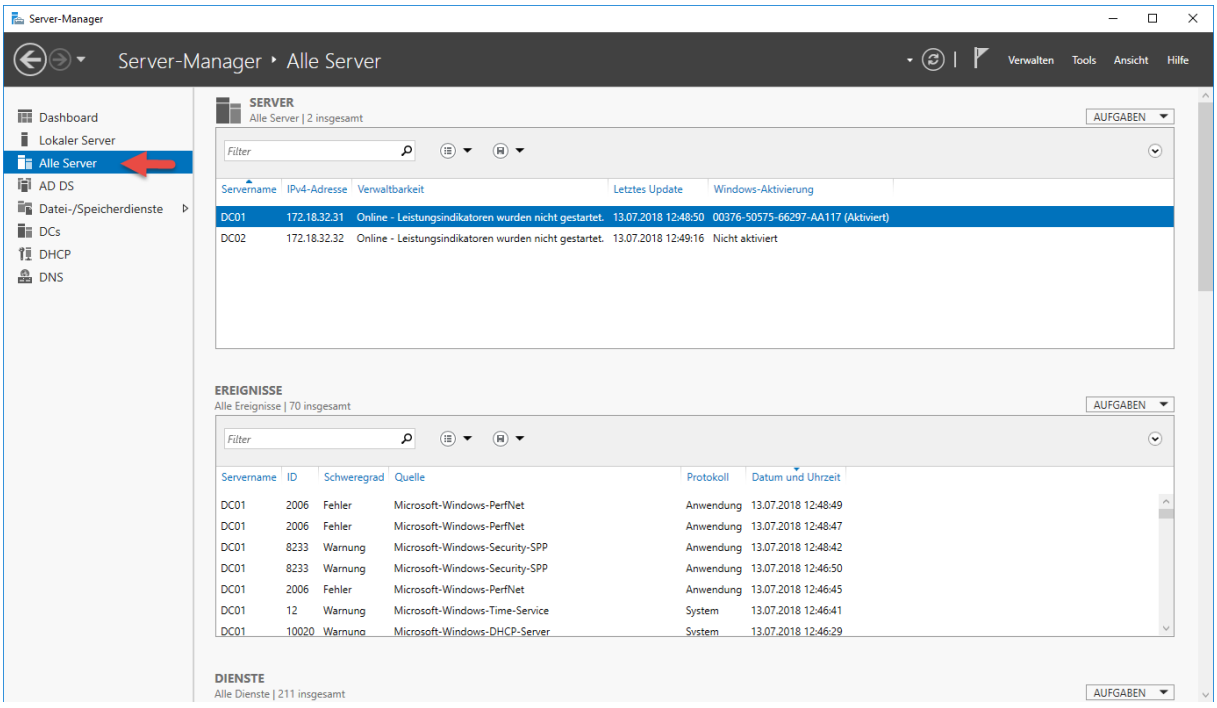
- Replikation lingering (Tombstone)
    - 1388,1988,2042
- Replikations DNS Lookup Probleme
    - 1925,2087,2088
- Replikations Konnektivitäts Probleme
    - 1925
- Replikations Topology Probleme
    - 1311

Active Directory Health-Check

Dashboard:



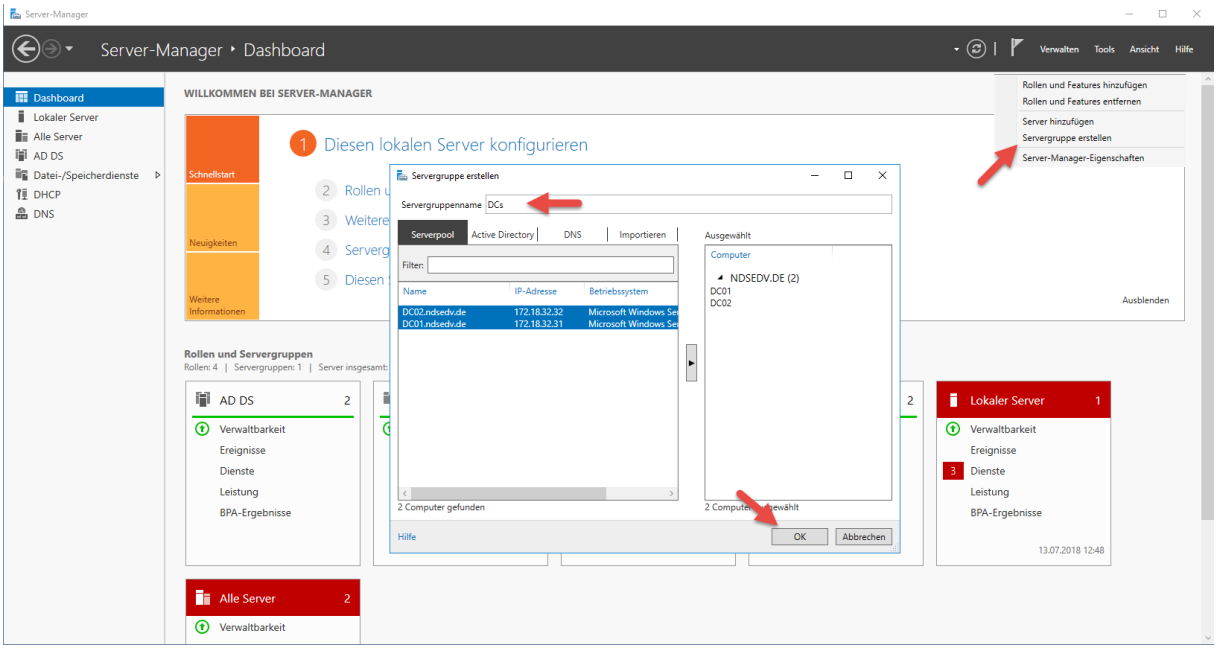
-Multiple Server



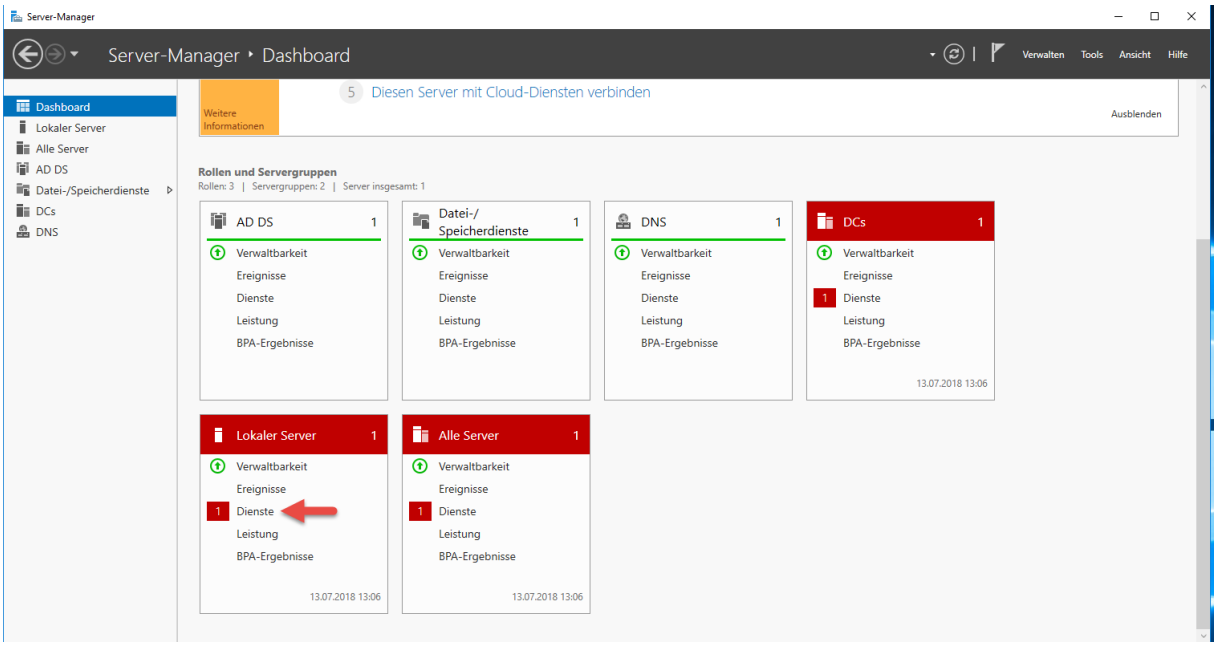
Erstellt von Jörn Walter **13.07.2018**

Active Directory Health-Check

-Server Gruppen



-Health Indikatoren

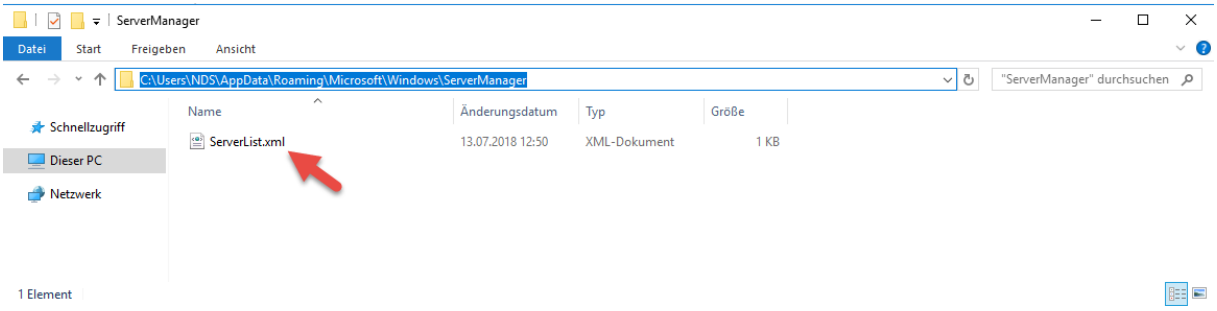


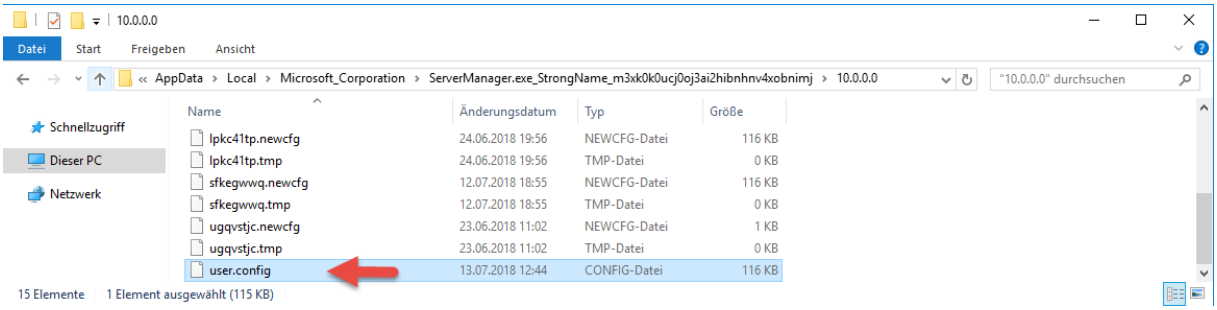
Erstellt von Jörn Walter **13.07.2018**

Active Directory Health-Check

-Export/Import

Export der Server Manager Einstellungen vom DC01:

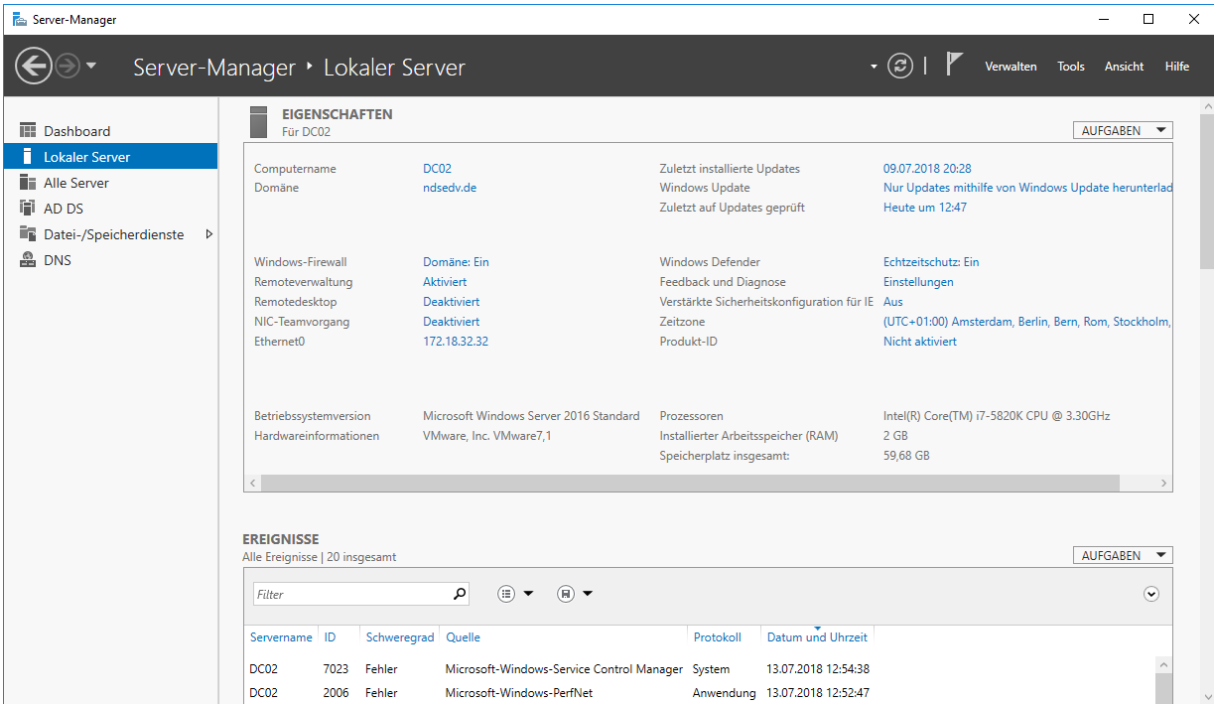




-Export/Import

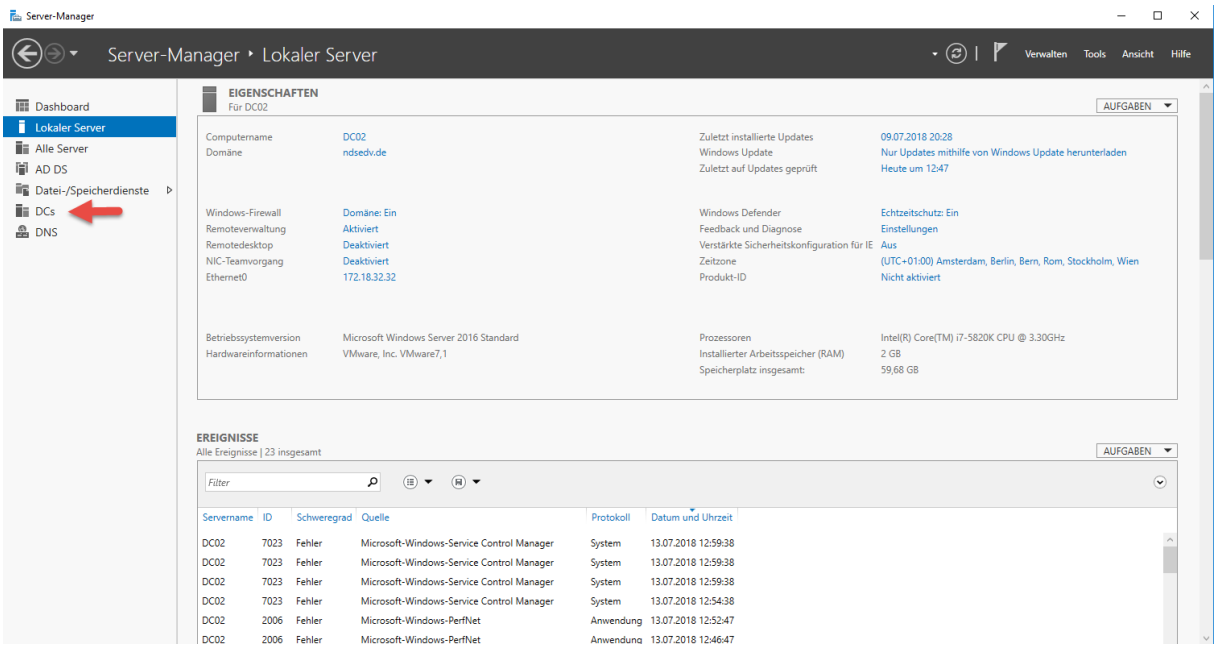
Import der Server Manager Einstellungen des DC01 auf DC02:

Ansicht vor dem Import der Einstellungen



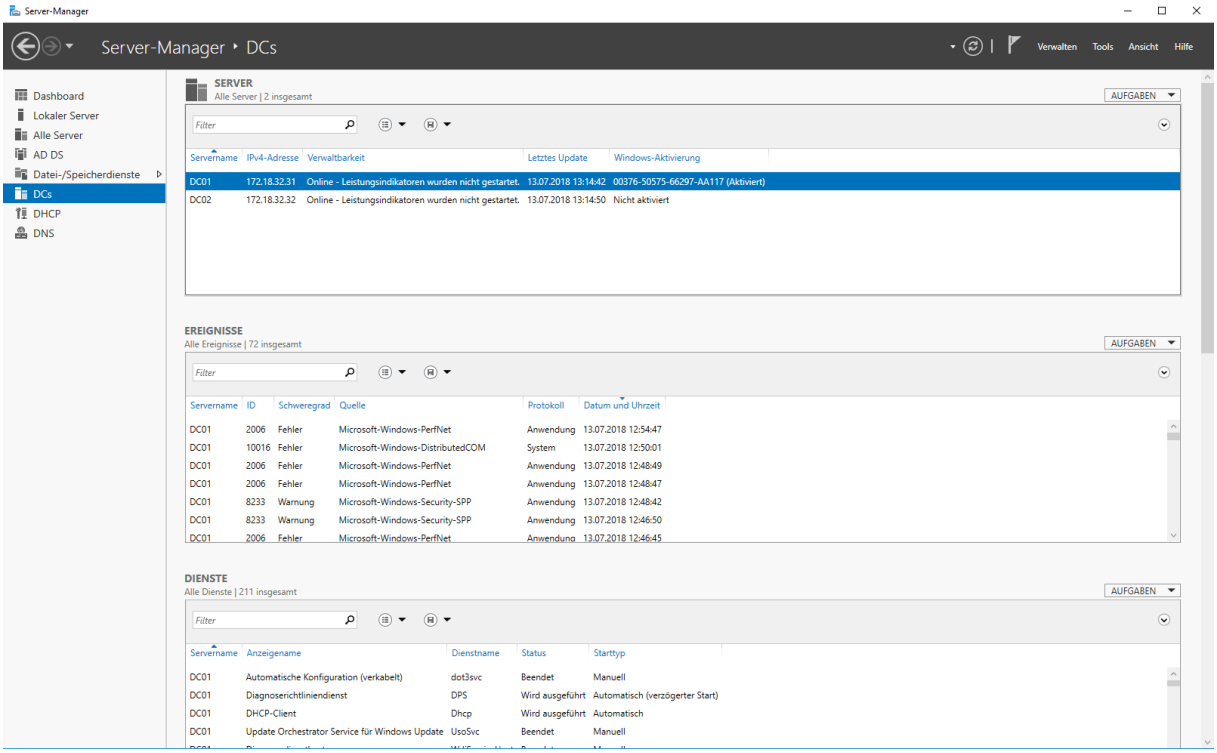
Active Directory Health-Check

Ansicht nach dem Import der Einstellungen



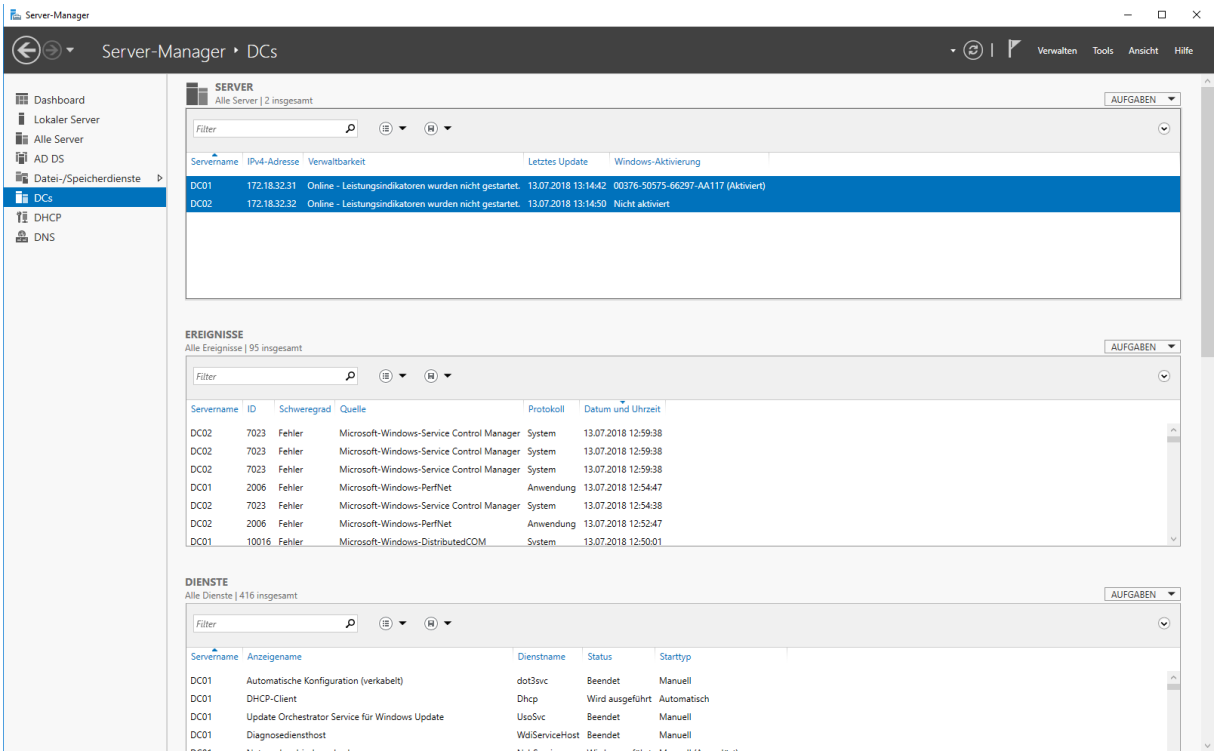
Events & Services

-Einzelansicht eines Servers

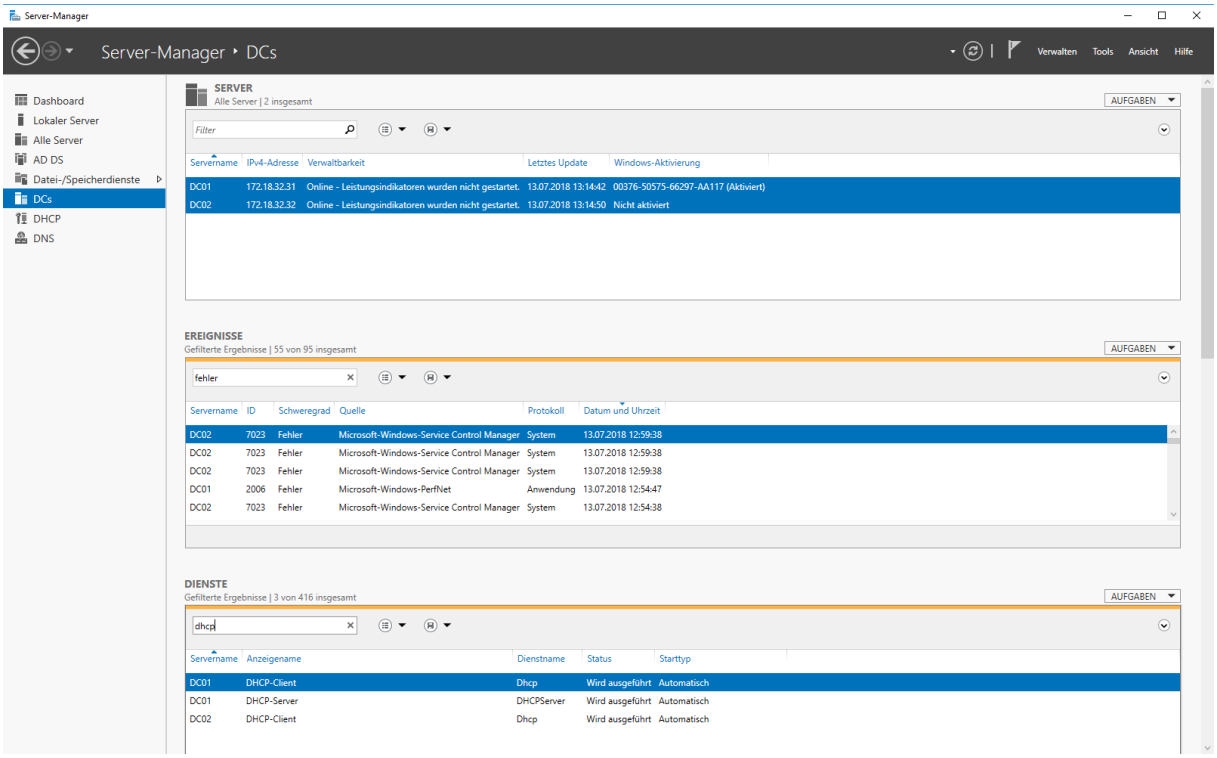


Active Directory Health-Check

-Gruppierte Ansicht zweier Server



-Gefilterte Ansicht



Erstellt von Jörn Walter **13.07.2018**

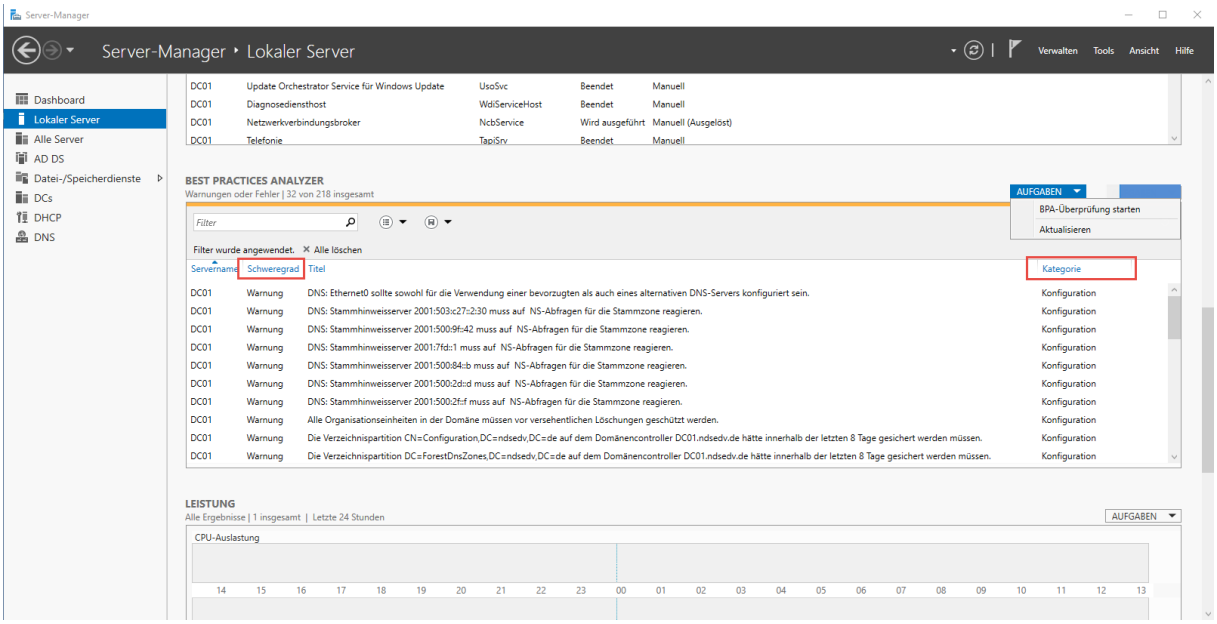
Active Directory Health-Check

Best Practice Analyzer:

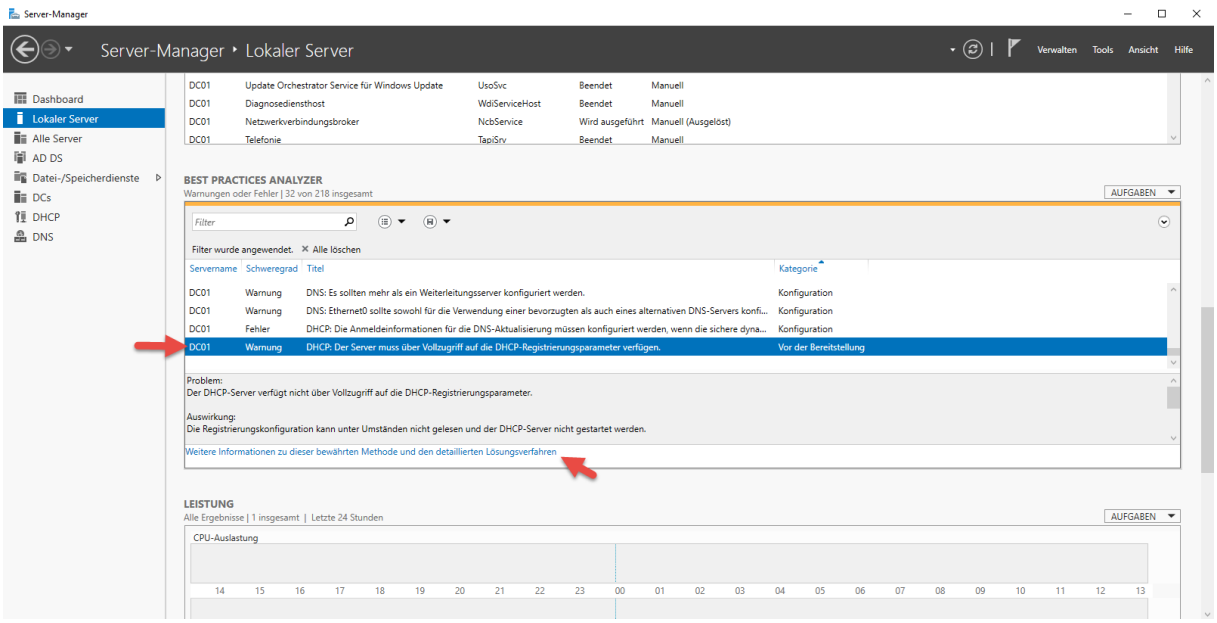
Die Rollen des Servers werden mit den Regeln zu bewährten Methoden verglichen und je nach Schweregrad des Verstoßes wird entweder ein Fehler eine Information oder eine Warnung ausgegeben.

Die Regeln lassen sich dabei in 8 Kategorien aufteilen:

- Sicherheit
- Leistung
- Konfiguration
- Richtlinie
- Vorgang
- Vor der Bereitstellung
- Nach der Bereitstellung
- Voraussetzungen



-Probleme ermitteln



Active Directory Health-Check

-Lösungen

Für die ermittelten Probleme werden auch Lösungen angeboten.

Resolution

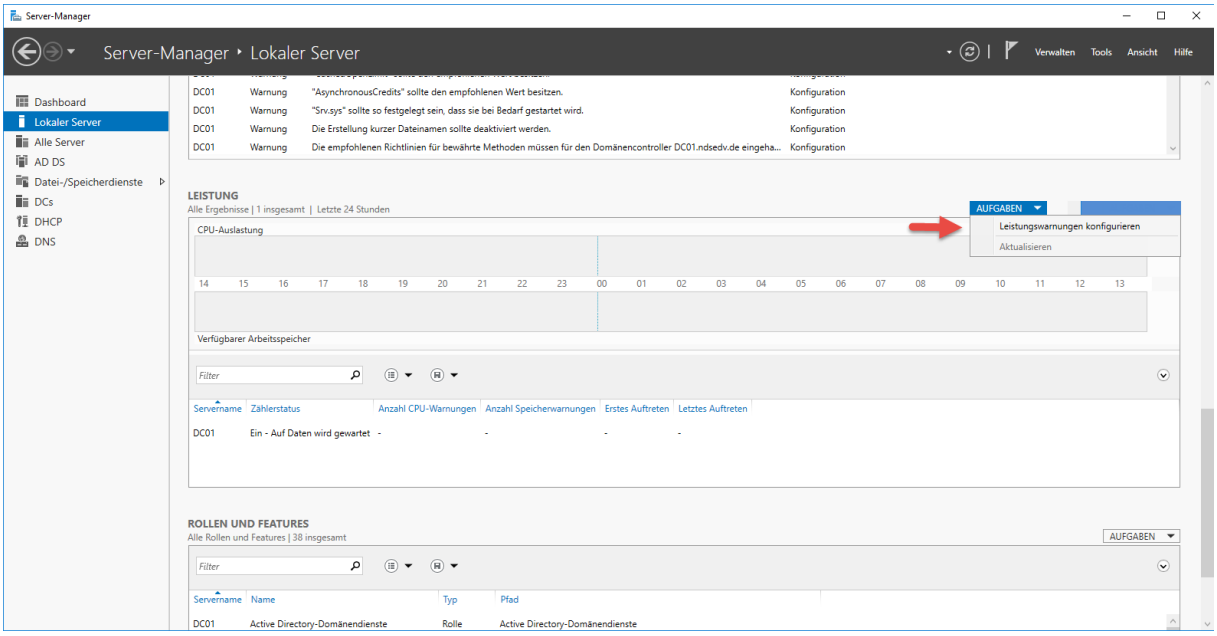
> *Assign the DHCPServer service full control permissions to the DHCP registry.*

To give DHCPServer service full control permissions to the DHCP registry

1. Click **Start**, type **regedit** in **Start Search**, click **Yes** in **User Account Control** if prompted, and then press **ENTER**.
2. In the registry tree, navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services\DHCPServer**.
3. Right-click **DHCPServer** and then click **Permissions**.
4. In **Group or User names** click **DHCPServer** if a DHCP Server is already present. Otherwise, click **Add** in **Select Users or Groups**.
5. Click **Locations** and select the hostname of the system, enter **NT Service\DHCPServer**, and then, click **OK**.
6. In **Permissions for DHCP Server** check **Allow** for **Full control** and then click **OK**.

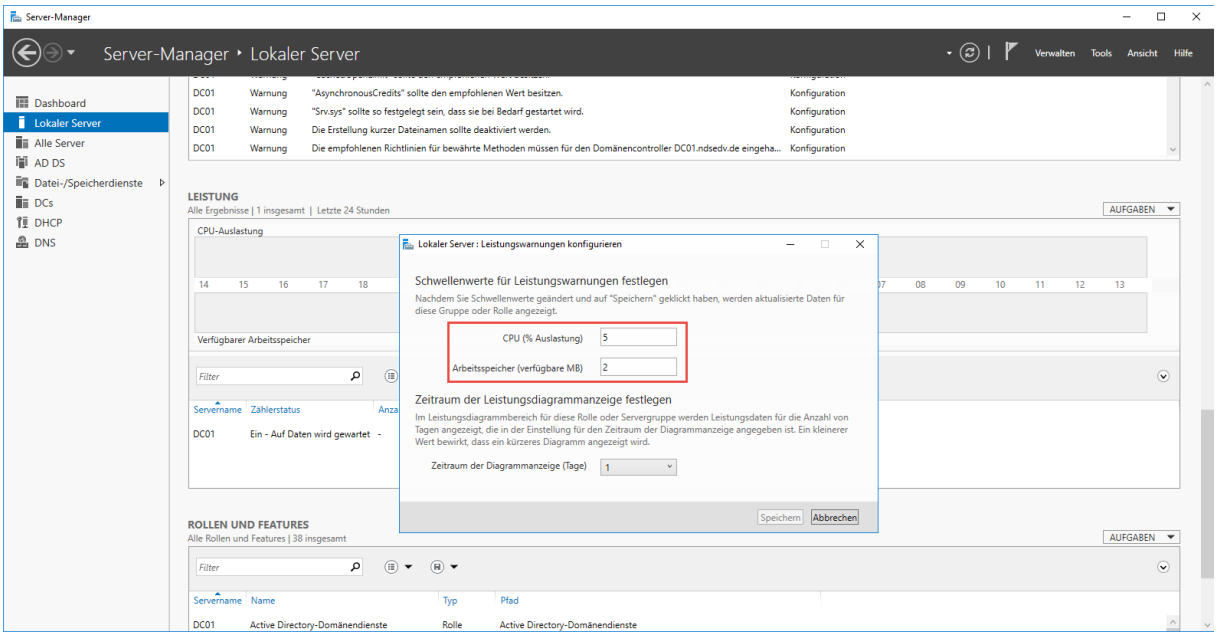
Performance:

-Leistungswarnungen



Active Directory Health-Check

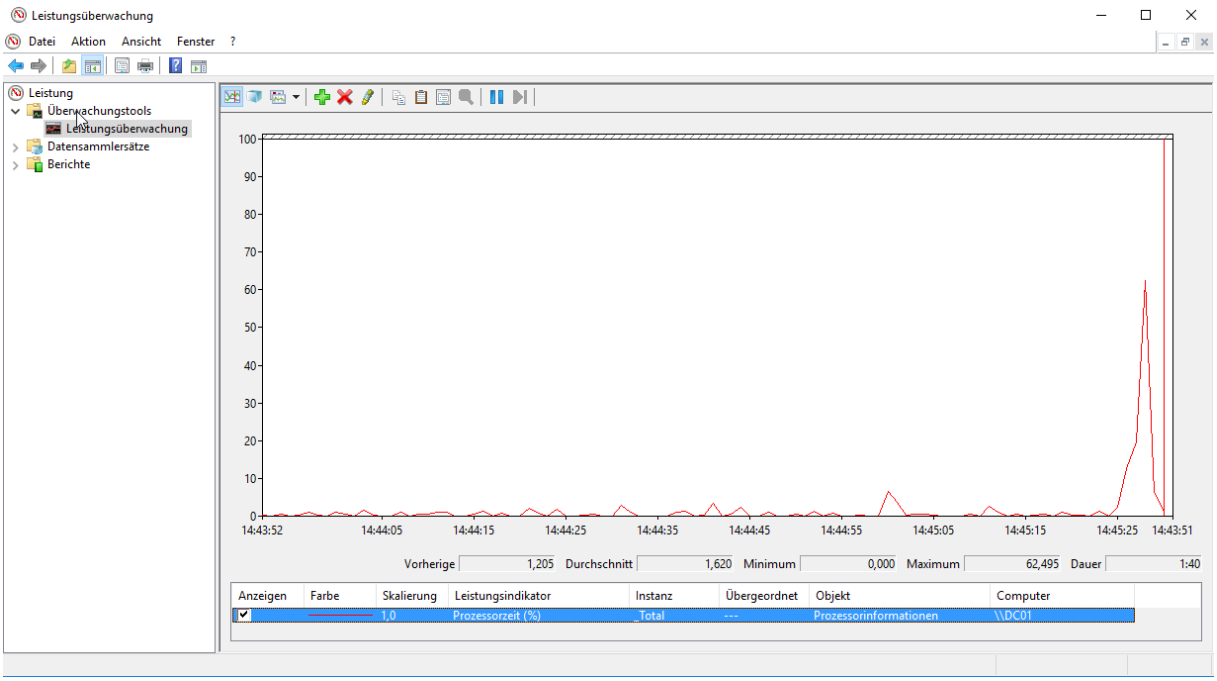
-Speicher & CPU



Diagnose Tool – Performance Monitor:

-Echzeitüberwachung

Die Leistungsüberwachung startet standardmäßig mit dem Indikator namens Prozessorzeit.



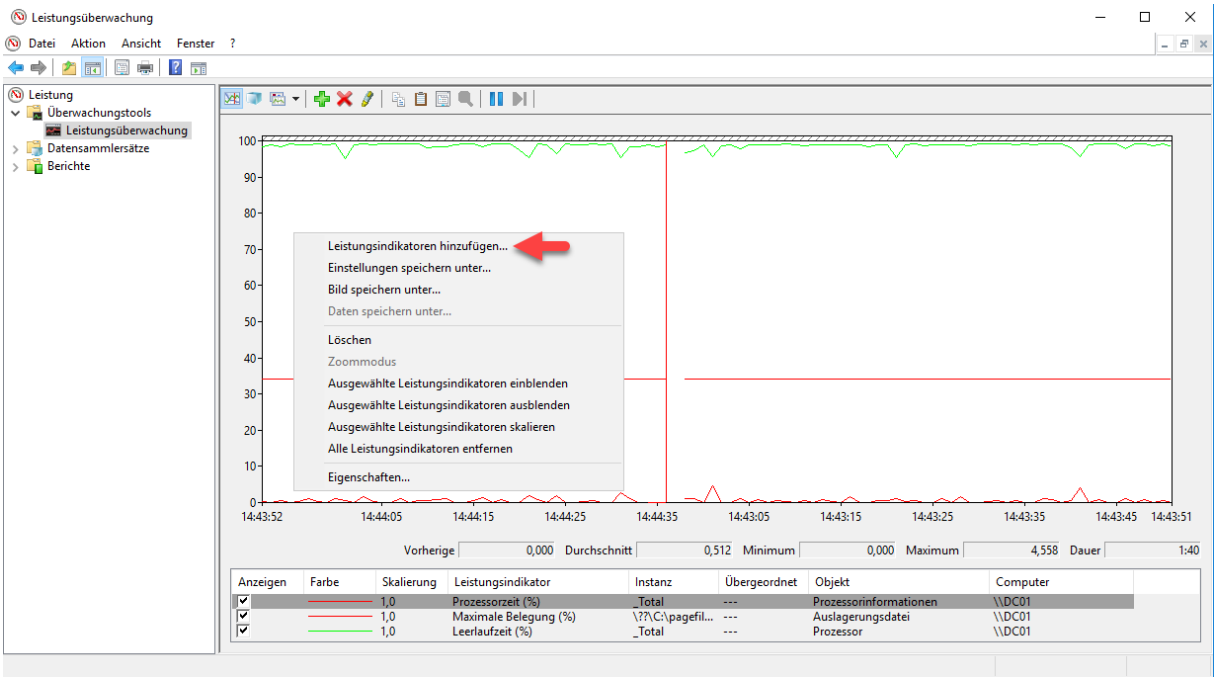
Erstellt von Jörn Walter **13.07.2018**

Active Directory Health-Check

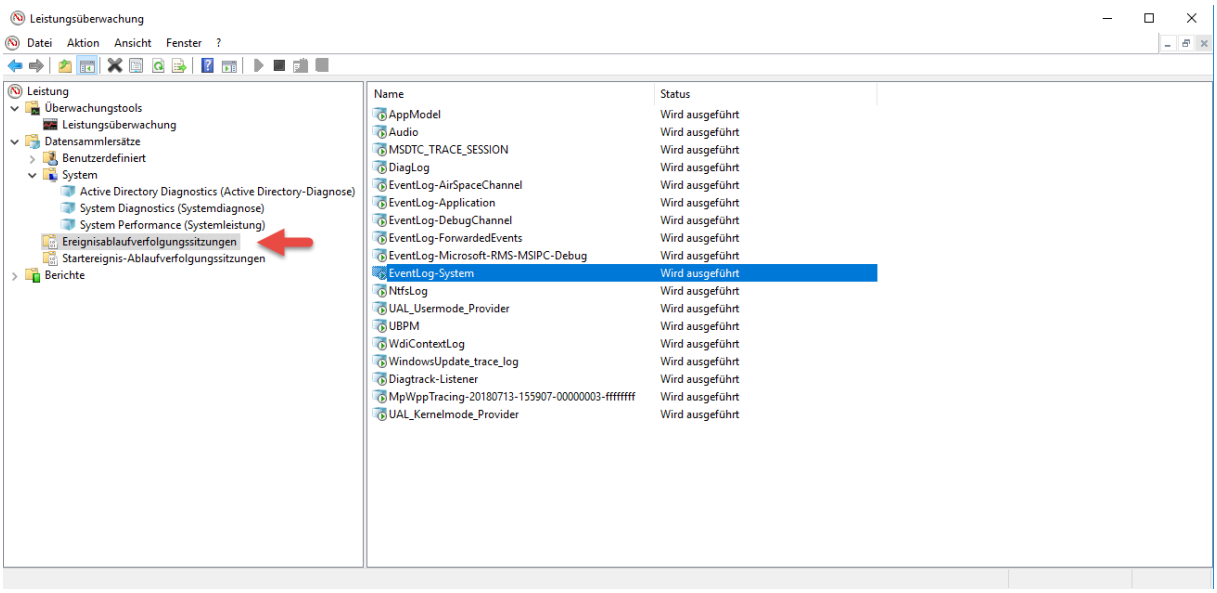
Datensammlersätze

-Leistungsindikatoren

Weitere Indikatoren können über einen Rechtsklick zur Analyse hinzugefügt werden.



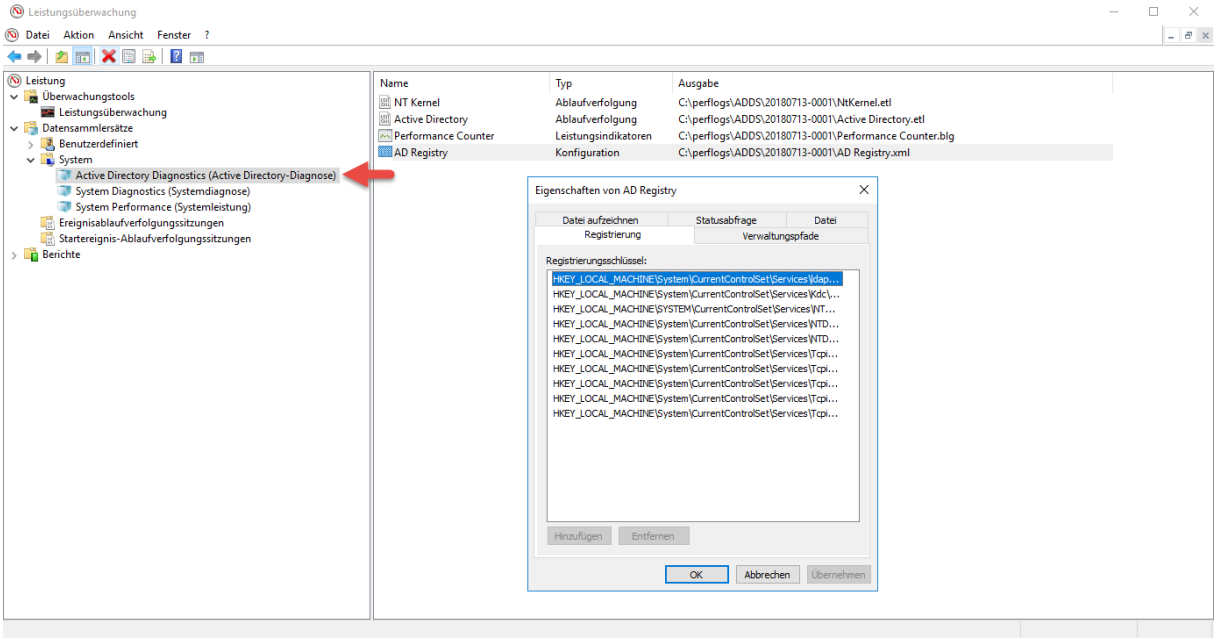
-Ereignisablaufverfolgung



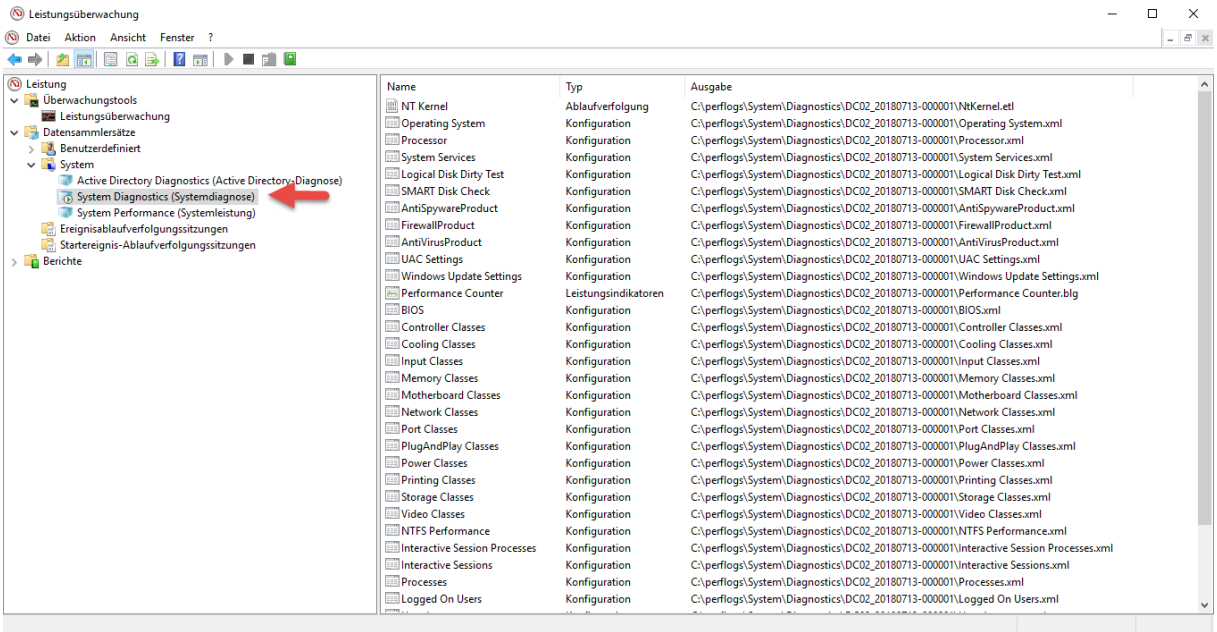
Active Directory Health-Check

-Systemkonfigurationsinformationen

Prüfung der Einträge in der Active Directory Registry



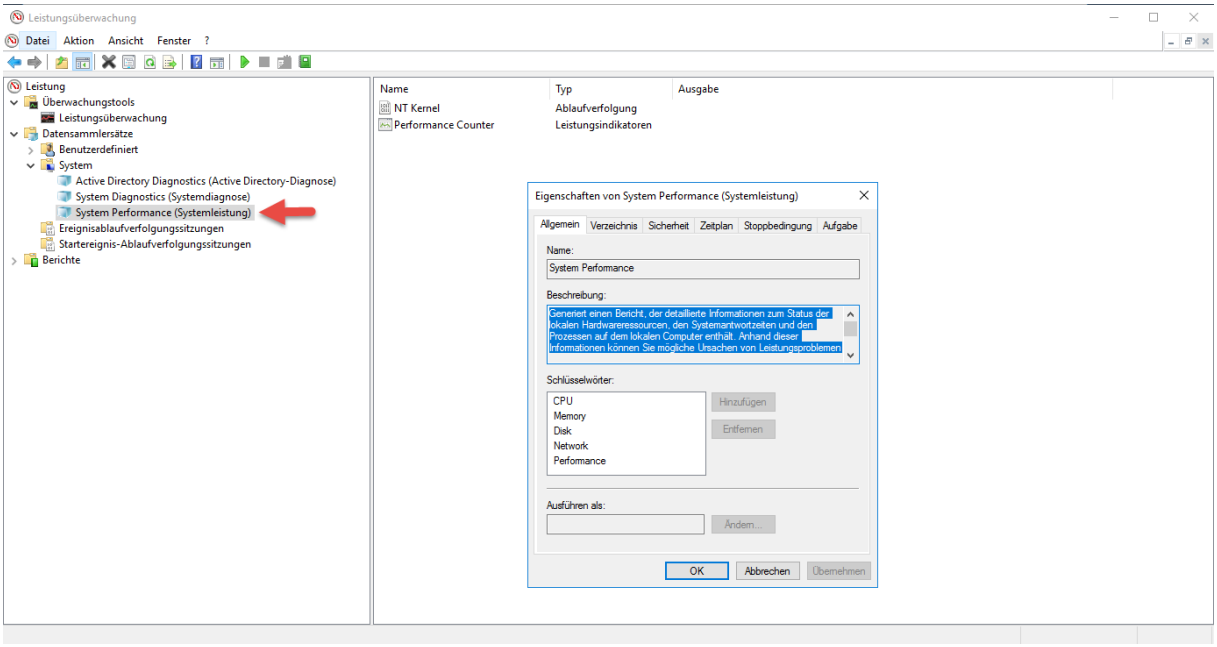
Prüfung des gesamten Systems



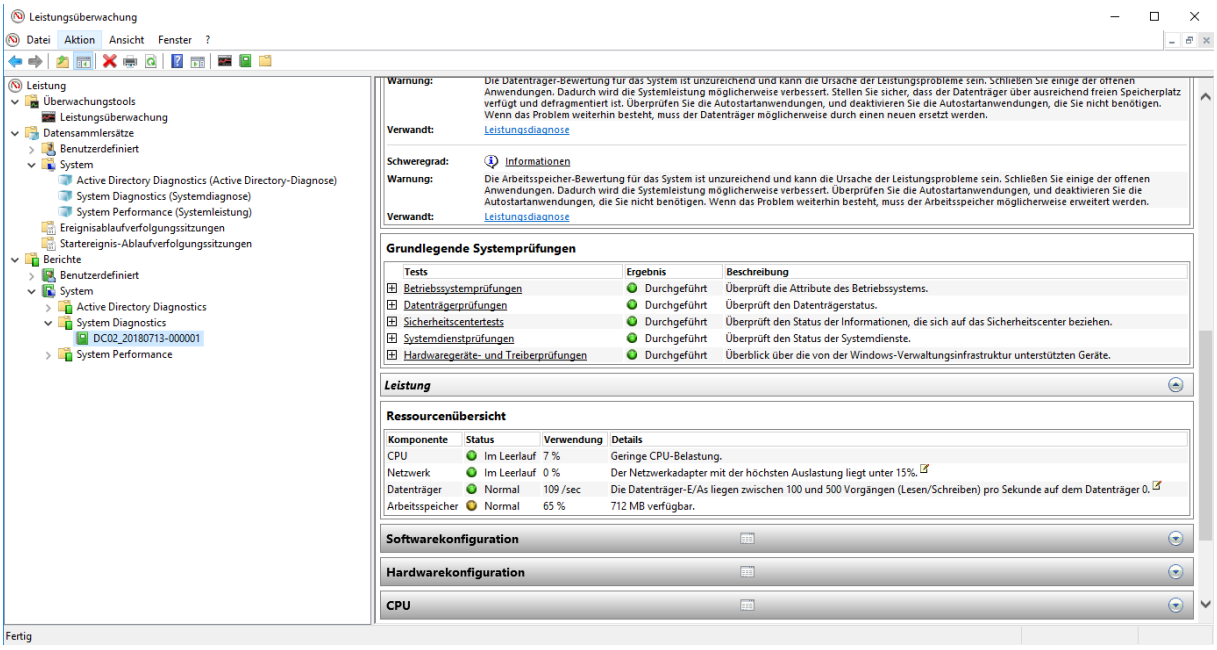
Erstellt von Jörn Walter **13.07.2018**

Active Directory Health-Check

Prüfung der Systemperformance



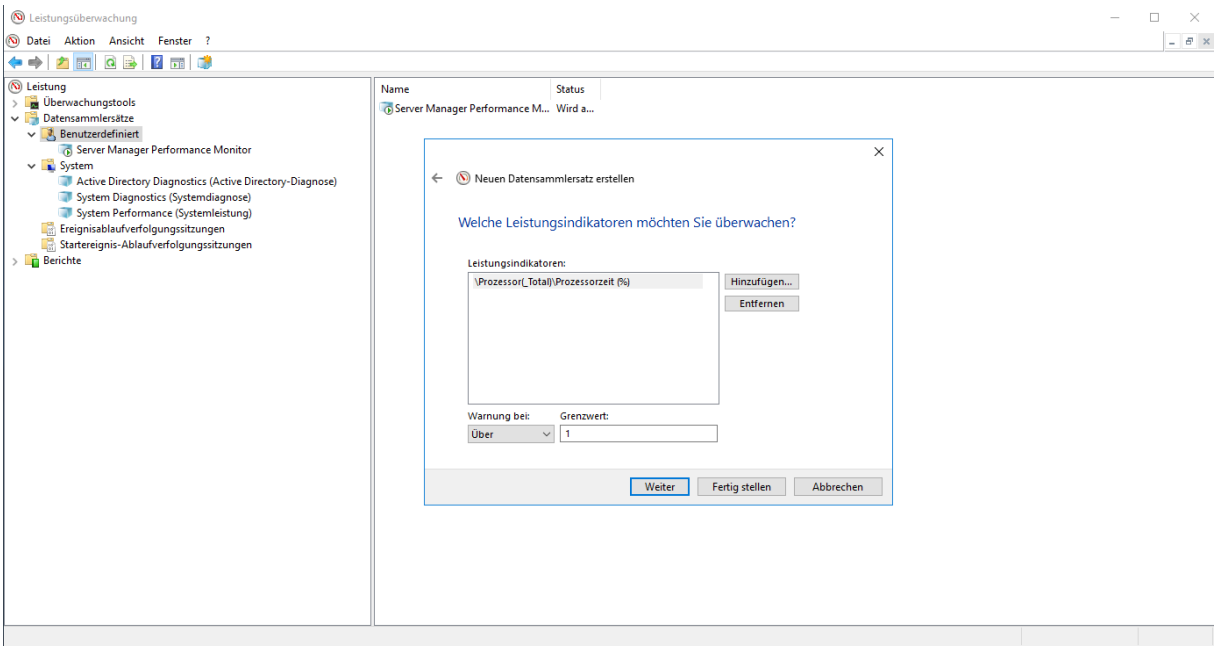
-Systemkonfigurationsinformations-Bericht



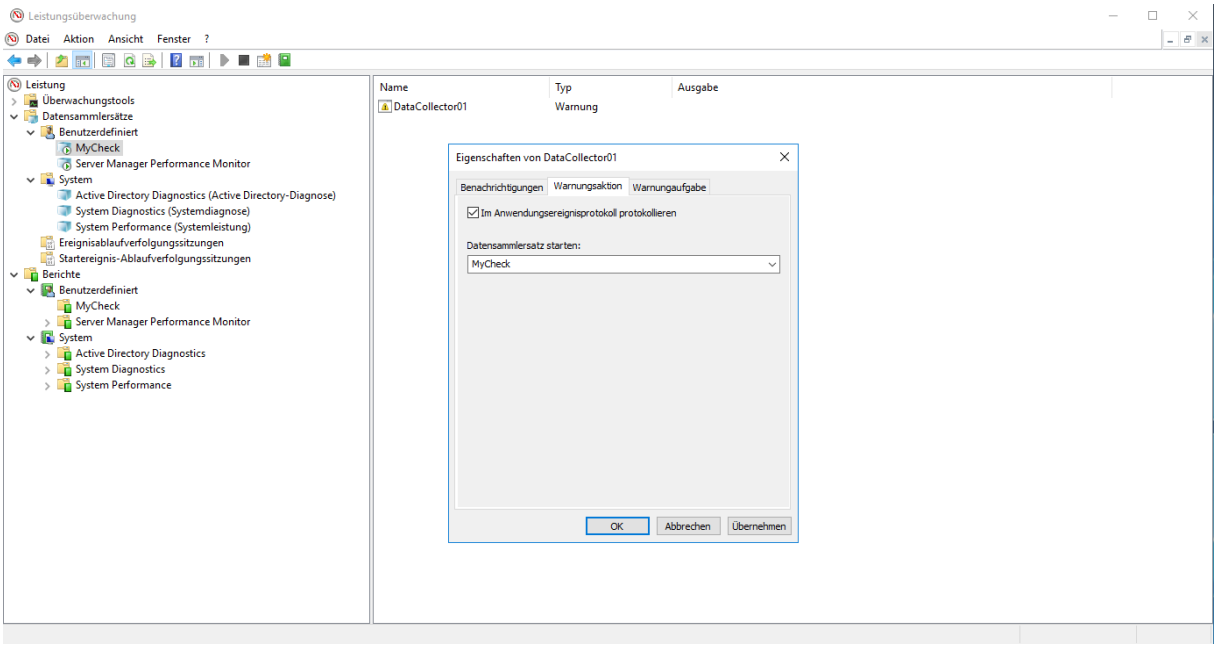
Active Directory Health-Check

Warnungen:

Es lassen sich Warnungen ins Protokoll schreiben



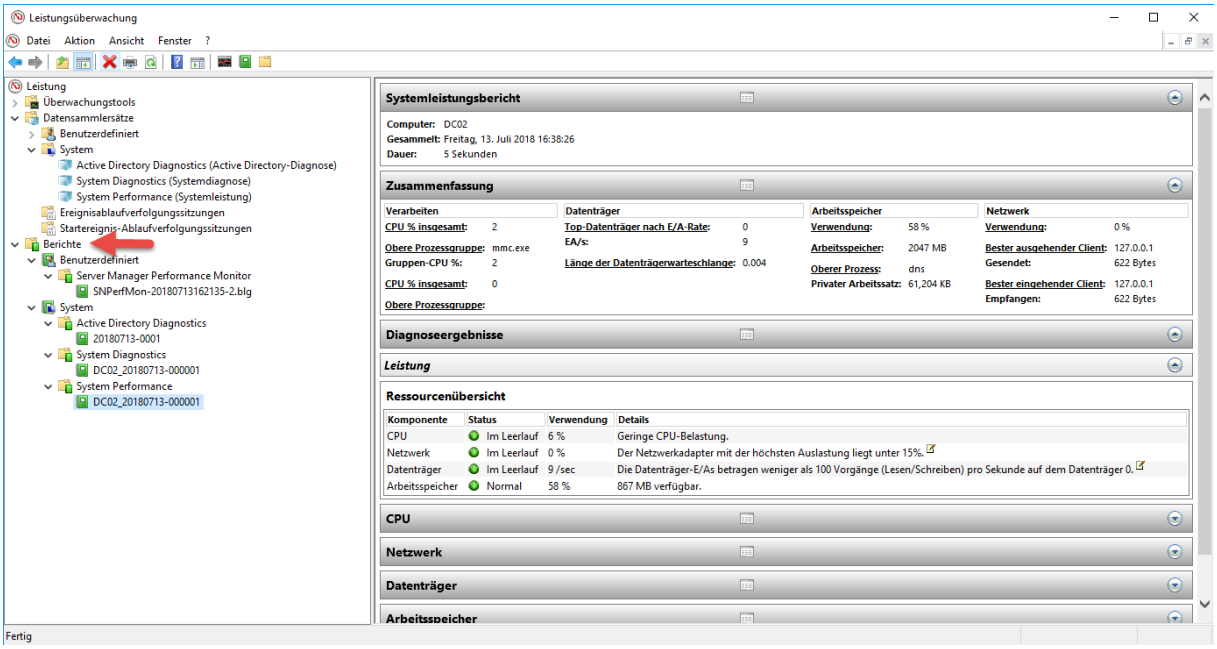
Aktionen lassen sich auf Warnungen ausführen



Active Directory Health-Check

Berichte:

Sobald eine Überprüfung gestartet wurde, wird dazu ein Bericht erstellt. Zusammengefasst finden wir diese unter Berichte.

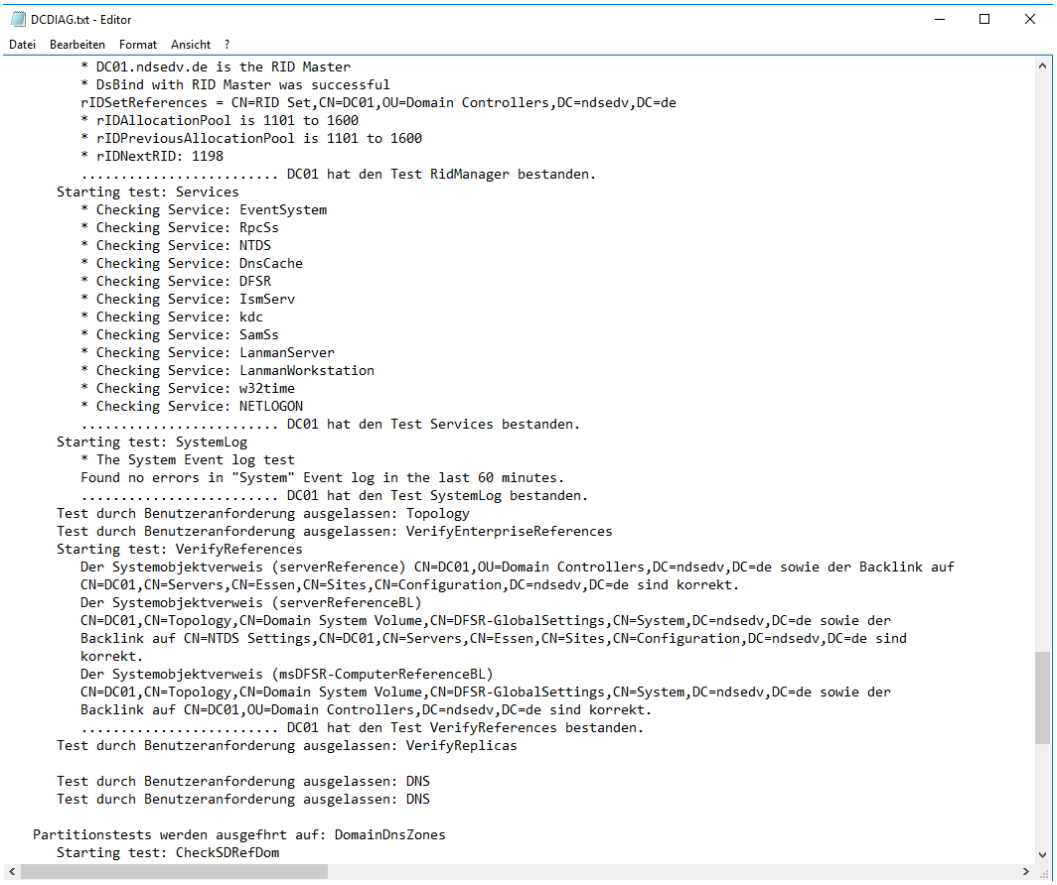


Diagnose Tool – DCDIAG:

- Schalterfunktionen
  - /a gibt eine Liste aller getesteten DCs aus einer Site aus
  - /e gibt eine Liste aller getesteten DCs aus der Gesamtstruktur aus
  - /c ausführlicher Test inkl. DNS
  - /d Debug Modus
  - /f :LogFile
  - /q gibt nur Fehler aus
  - /s definiert einen DC
  - /u startet den Test mit einem alternativen Benutzer
  - /test:DNS nur DNS Test
  - /v gibt alles aus nicht nur Fehler

Active Directory Health-Check

- Alle DCdiag Tests wurden erfolgreich bestanden
    - dcdiag /d /f:C:\Temp\DCDIAG.txt



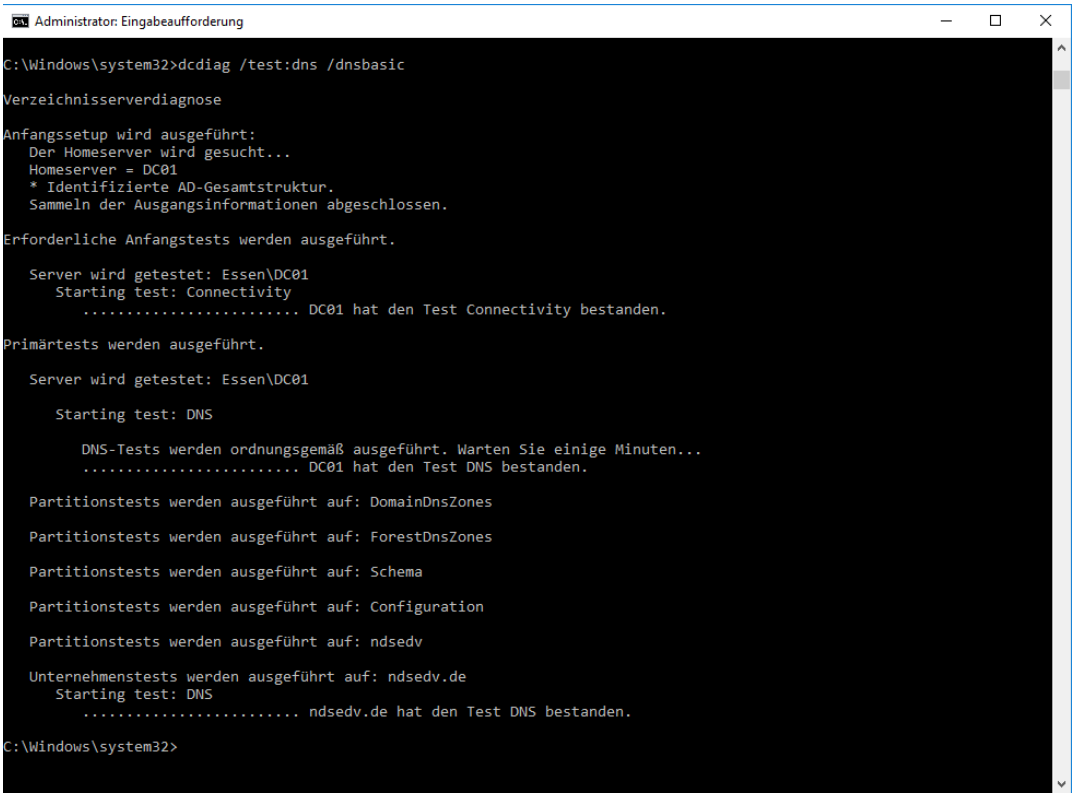
DCDIAG.txt - Editor

Datei Bearbeiten Format Ansicht ?

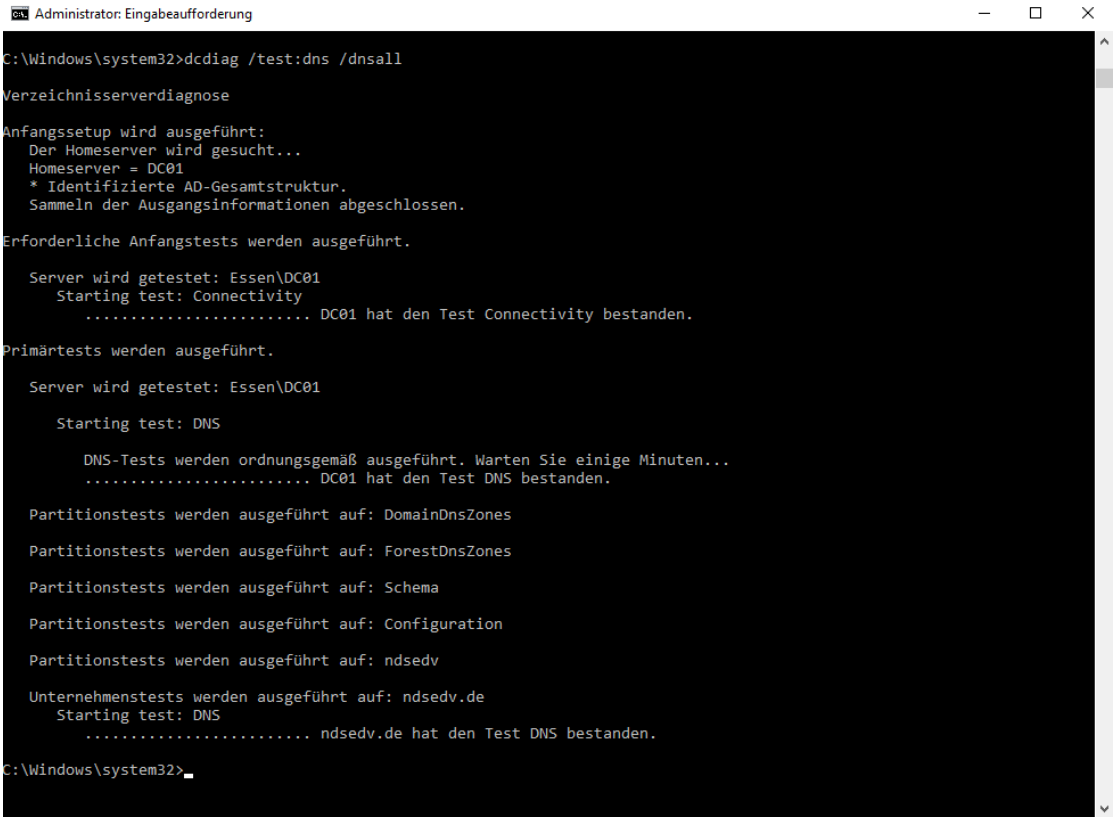
```
         * DC01.ndsedv.de is the RID Master
         * DsBind with RID Master was successful
         rIDSetReferences = CN=RID Set,CN=DC01,OU=Domain Controllers,DC=ndsedv,DC=de
         * rIDAllocationPool is 1101 to 1600
         * rIDPreviousAllocationPool is 1101 to 1600
         * rIDNextRID: 1198
         ..... DC01 hat den Test RidManager bestanden.
      Starting test: Services
         * Checking Service: EventSystem
         * Checking Service: RpcSs
         * Checking Service: NTDS
         * Checking Service: DnsCache
         * Checking Service: DFSR
         * Checking Service: IsmServ
         * Checking Service: kdc
         * Checking Service: SamSs
         * Checking Service: LanmanServer
         * Checking Service: LanmanWorkstation
         * Checking Service: w32time
         * Checking Service: NETLOGON
         ..... DC01 hat den Test Services bestanden.
      Starting test: SystemLog
         * The System Event log test
         Found no errors in "System" Event log in the last 60 minutes.
         ..... DC01 hat den Test SystemLog bestanden.
      Test durch Benutzeranforderung ausgelassen: Topology
      Test durch Benutzeranforderung ausgelassen: VerifyEnterpriseReferences
      Starting test: VerifyReferences
         Der Systemobjektverweis (serverReference) CN=DC01,OU=Domain Controllers,DC=ndsedv,DC=de sowie der Backlink auf
         CN=DC01,CN=Servers,CN=Essen,CN=Sites,CN=Configuration,DC=ndsedv,DC=de sind korrekt.
         Der Systemobjektverweis (serverReferenceBL)
         CN=DC01,CN=Topology,CN=Domain System Volume,CN=DFSR-GlobalSettings,CN=System,DC=ndsedv,DC=de sowie der
         Backlink auf CN=NTDS Settings,CN=DC01,CN=Servers,CN=Essen,CN=Sites,CN=Configuration,DC=ndsedv,DC=de sind
         korrekt.
         Der Systemobjektverweis (msDFSR-ComputerReferenceBL)
         CN=DC01,CN=Topology,CN=Domain System Volume,CN=DFSR-GlobalSettings,CN=System,DC=ndsedv,DC=de sowie der
         Backlink auf CN=DC01,OU=Domain Controllers,DC=ndsedv,DC=de sind korrekt.
         ..... DC01 hat den Test VerifyReferences bestanden.
      Test durch Benutzeranforderung ausgelassen: VerifyReplicas

      Test durch Benutzeranforderung ausgelassen: DNS
      Test durch Benutzeranforderung ausgelassen: DNS

   Partitionstests werden ausgefhrt auf: DomainDnsZones
      Starting test: CheckSDRefDom
```

Active Directory Health-Check

- DNS Basis Test
  - DCdiag /test:dns /dnsbasic



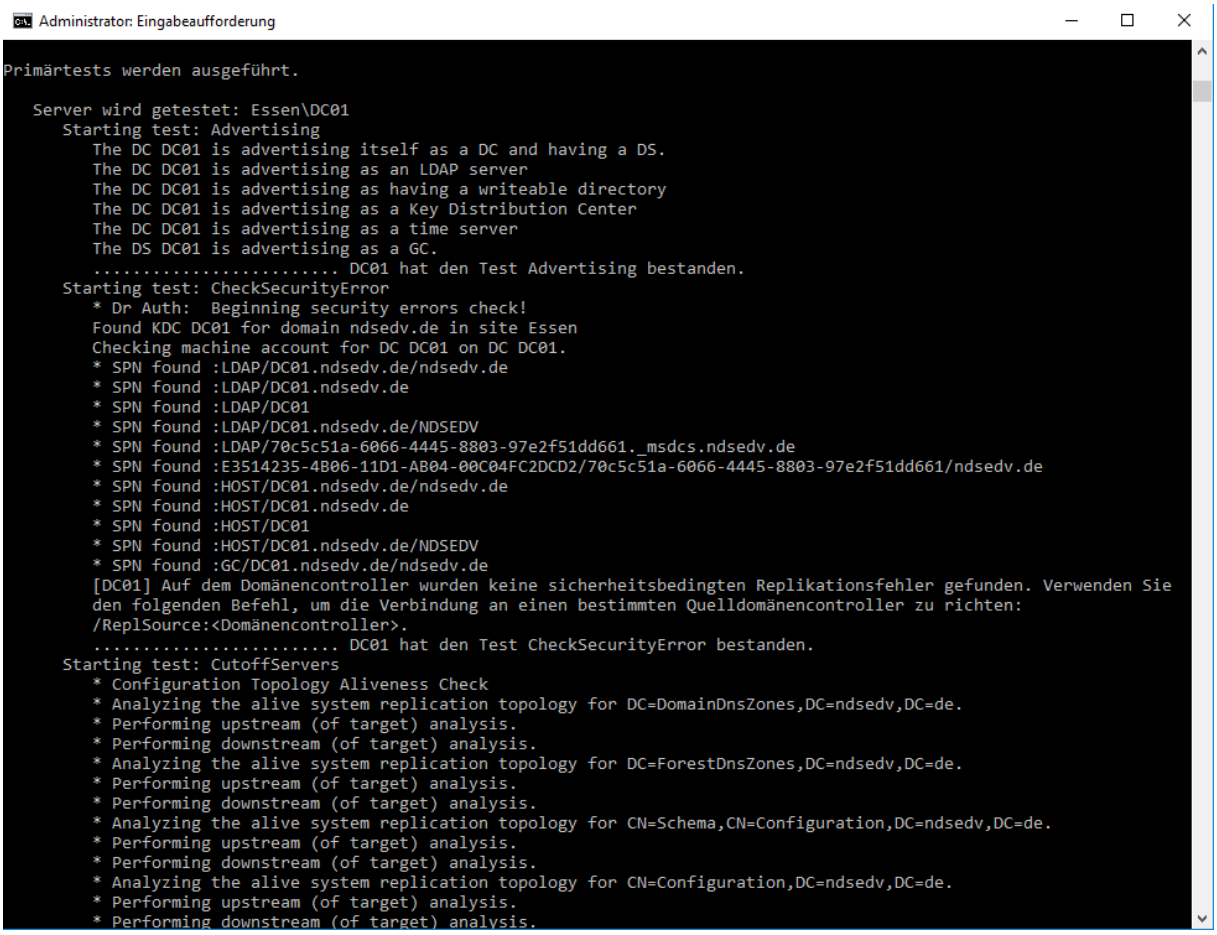
  - DCdiag /test:dns /dnsall



Net stop "dns client" & net start "dns client" & dcdiag /test:verifyreplicas /s:DC01

Active Directory Health-Check

- Dcdiag analysiert den Status von Domänencontrollern in einer Gesamtstruktur oder einem Unternehmen und meldet Probleme, die bei der Fehlerbehebung hilfreich sein können
    - dcdiag /c /e /v

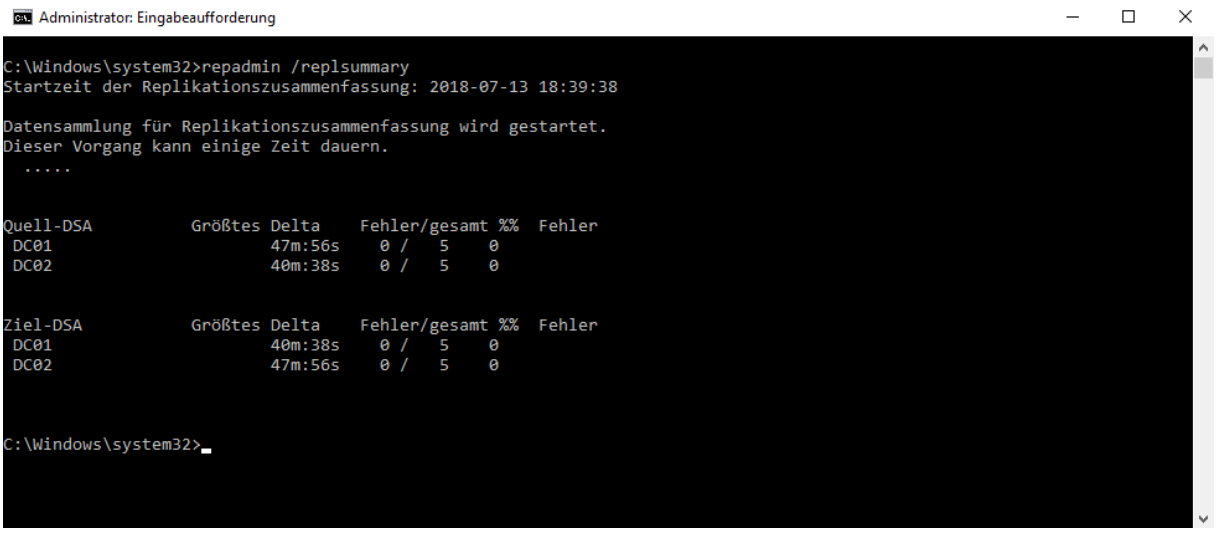


Active Directory Health-Check

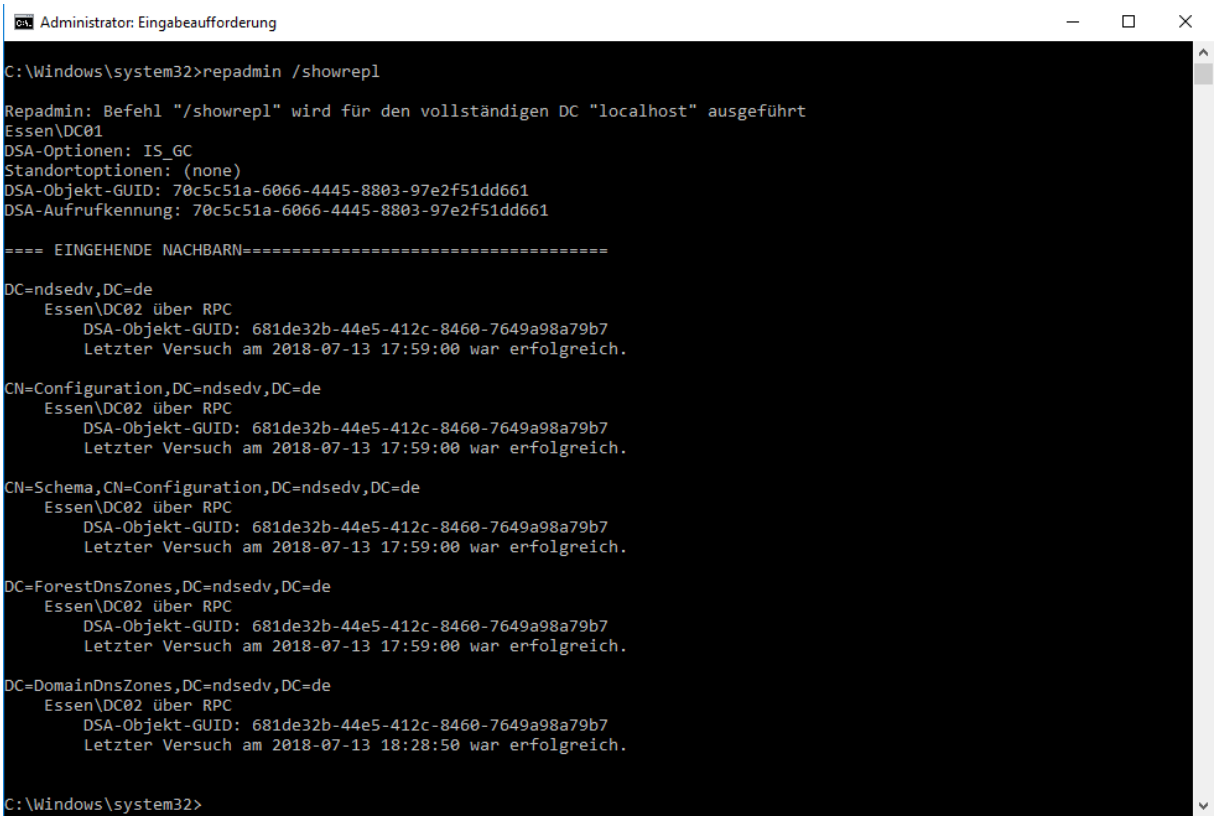
Diagnose Tool – Repadmin:

- Schalterfunktionen Übersicht
  - /replsummary
  - /showrepl
  - /queue
- Schalterfunktion Replikation
  - /syncall
  - /replicate

Zeigt eine Zusammenfassung



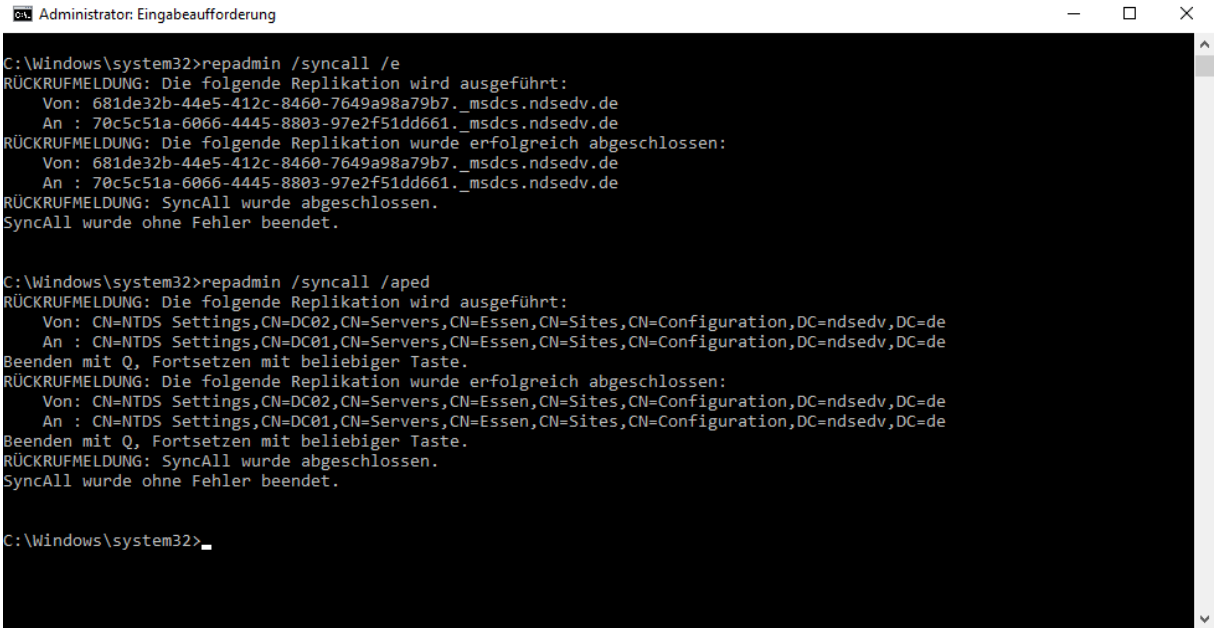
Zeigt die Objekte an



Optional: Weitere wichtige Schalterfunktionen:

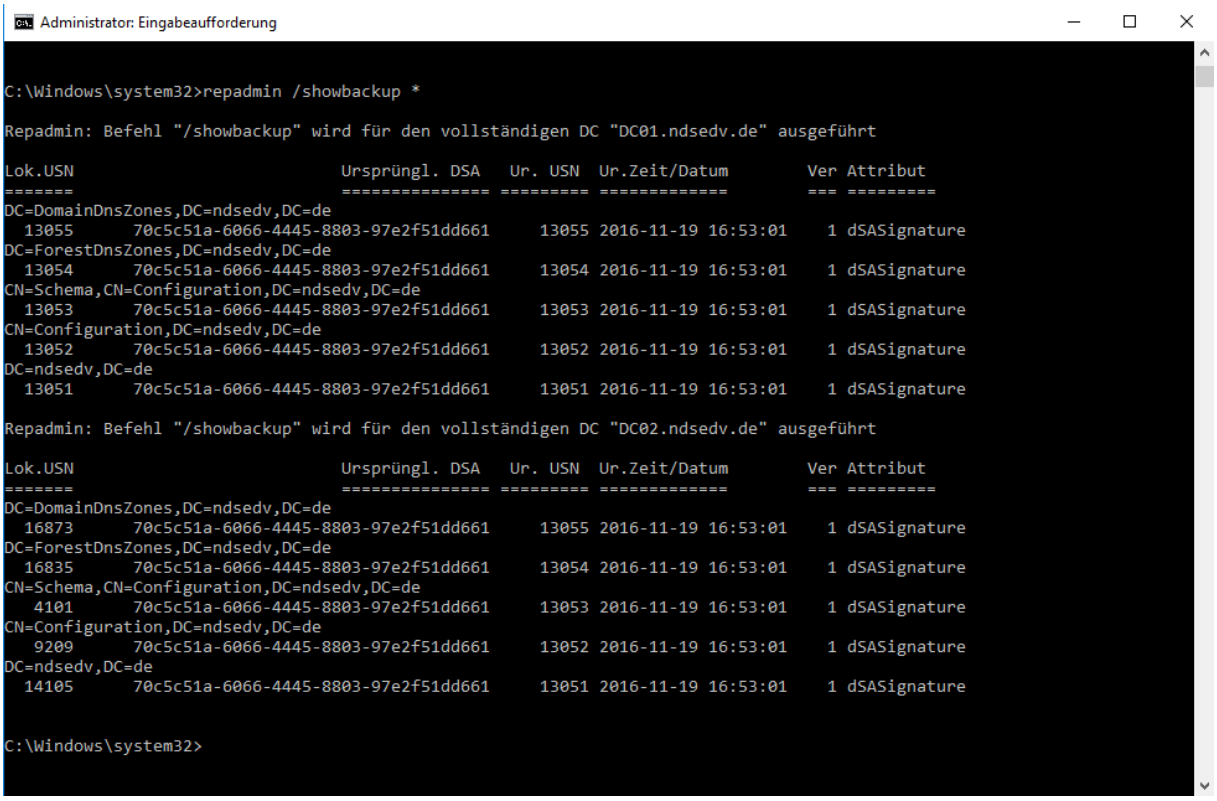
- Synchronisiert einen angegebenen Domänencontroller mit allen Replikationspartnern und meldet, wenn die Synchronisierung ausgeführt wurde.
    - repadmin /syncall /e
    - repadmin /syncall /aped

A (Alle Partitionen) P (Push) E (Enterprise) D (Distinguished Name)

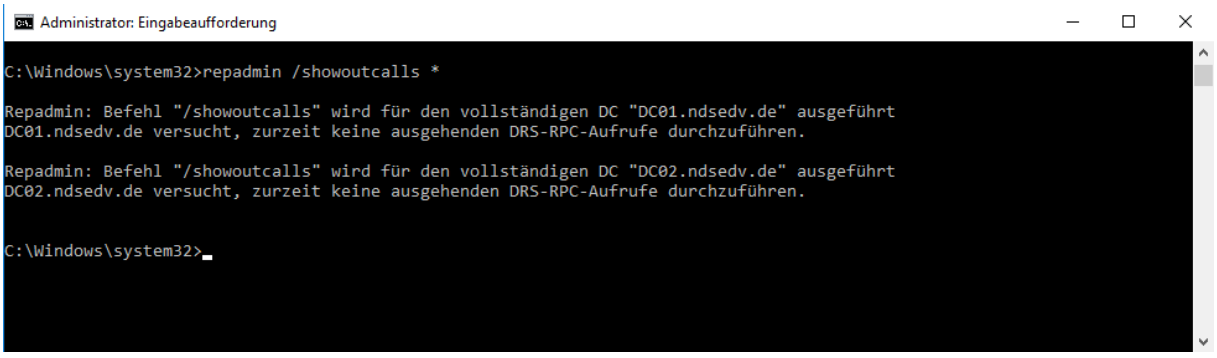


- Erzwingt, dass der KCC auf den Zieldomänencontrollern seine eingehende Replikationstopologie sofort neu berechnet
    - repadmin /kcc *

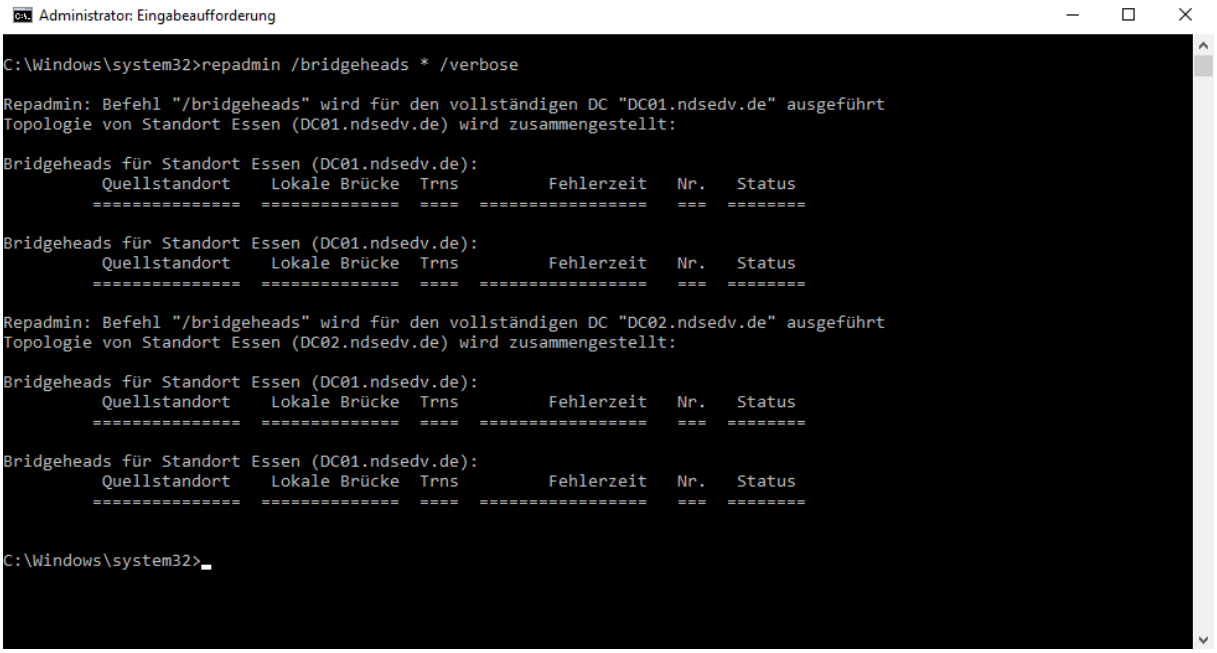
- Sucht nach dem letzten Mal, dass die DCs gesichert wurden, indem das DSASignature-Attribut von allen Servern eingelesen wird
    - repadmin /showbackup *



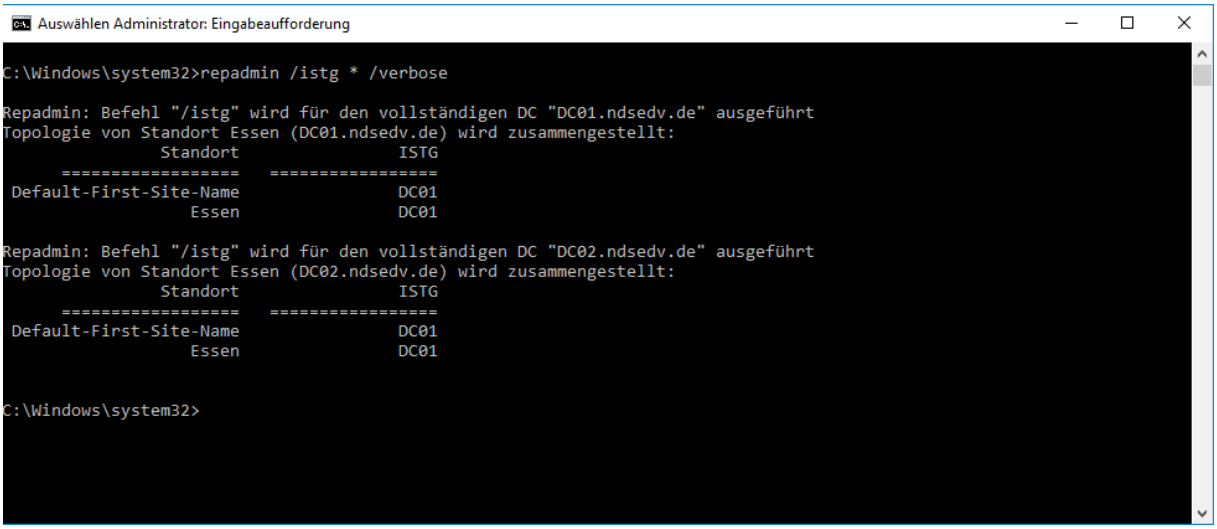
- Zeigt Aufrufe an, die noch nicht beantwortet wurden und vom angegebenen Server an andere Server gesendet wurden
    - repadmin /showoutcalls *



- Listet die Topologie-Informationen aller Bridgeheadserver auf wenn vorhanden
  - repadmin /bridgeheads * /verbose



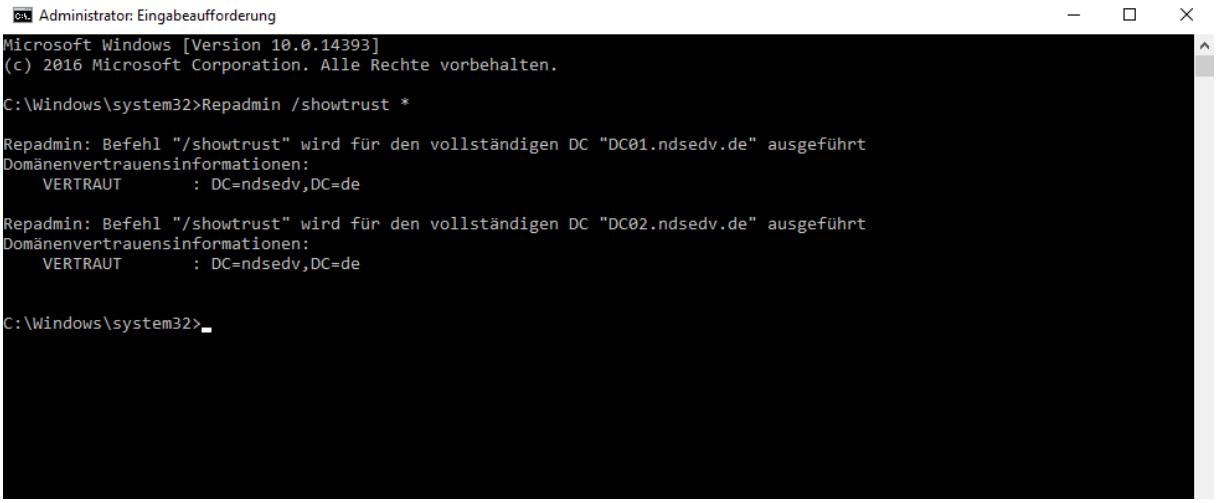
- Bericht über die Inter Site Topology
  - repadmin /istg * /verbose



Active Directory Health-Check

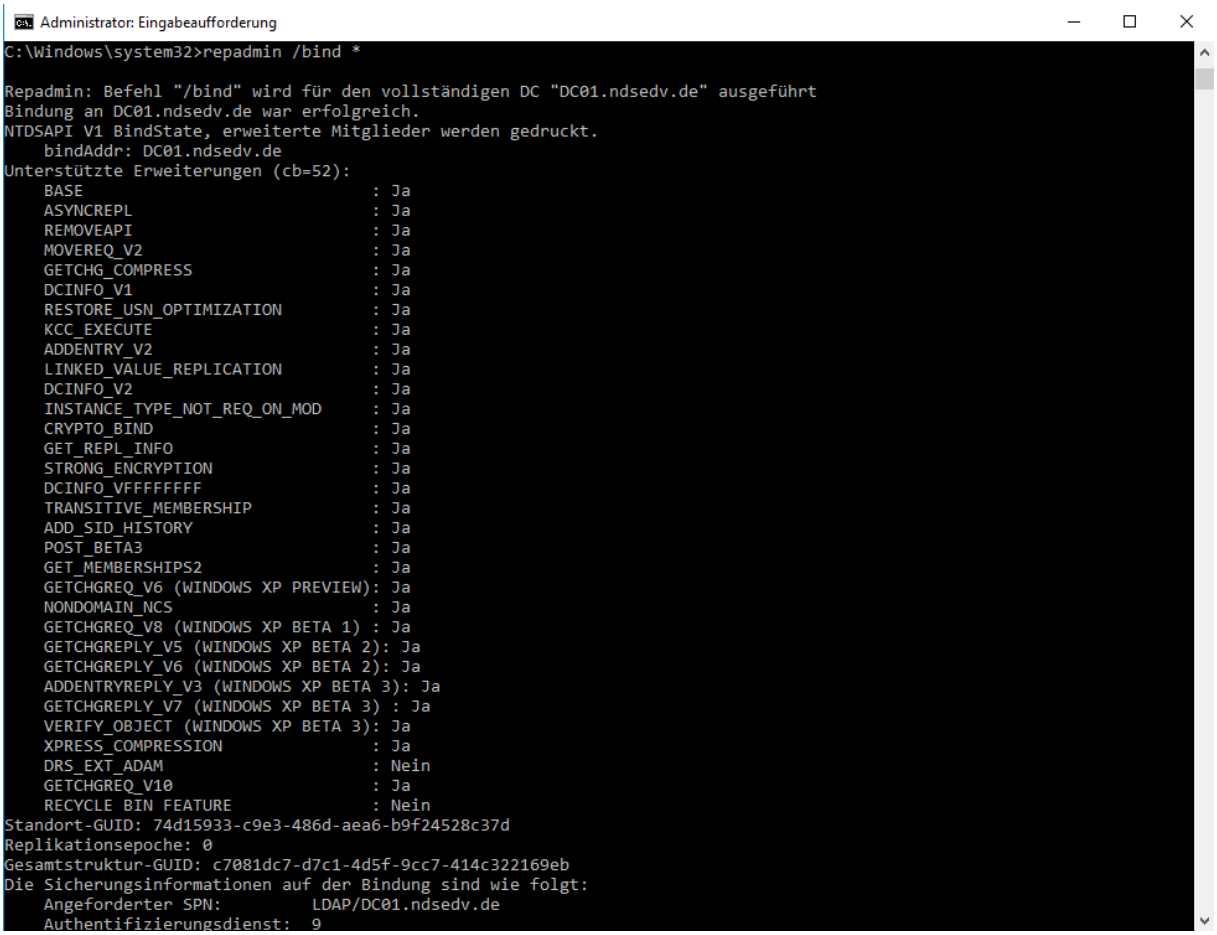
- Zeigt eine Liste von fehlgeschlagenen Replikationsereignissen an, die vom Knowledge Consistency Checker (KCC) erkannt wurden
    - repadmin /failcache *

- Listet alle Domänen auf, denen vertraut wird
    - repadmin /showtrust *



Active Directory Health-Check

- Zeigt die Replikationsfunktionen einer Verzeichnispartition an
    - repadmin /bind *



EventLog

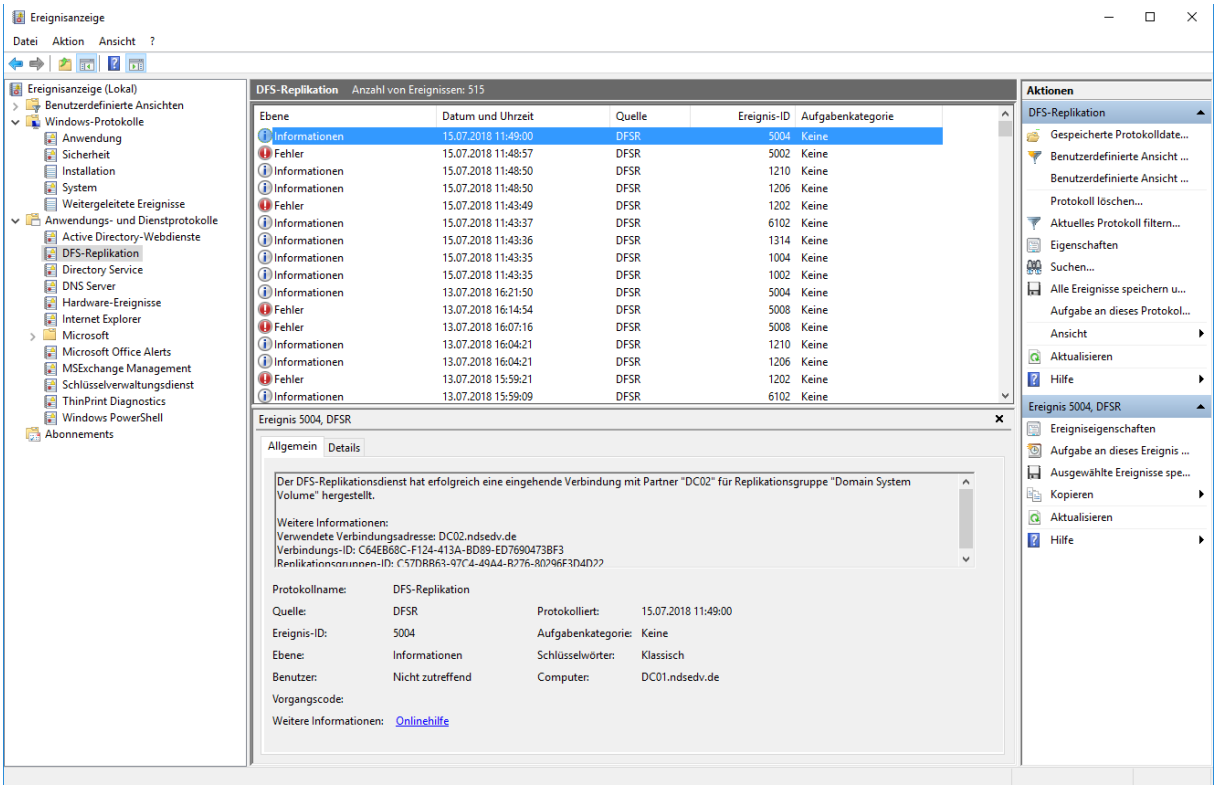
- Ereignis ID 1388
    - Ein totes Objekt (Tombstone) sollte mit dem Ziel DC repliziert werden
- Ereignis ID 1988
    - Ein totes Objekt wurde auf der Verzeichnispartition blockiert bevor es repliziert werden konnte
- Ereignis ID 2042
    - Der DC wurde schon zu lange nicht mehr repliziert

- Ereignis ID 1925
    - Beheben eines Verbindungsproblems bei der Replikation
- Ereignis 2087
    - Ein DNS Lookup Problem verursacht einen Replikationsfehler
- Ereignis ID 2088
    - Es ist ein DNS Lookup Problem bei erfolgreicher Replikation aufgetreten

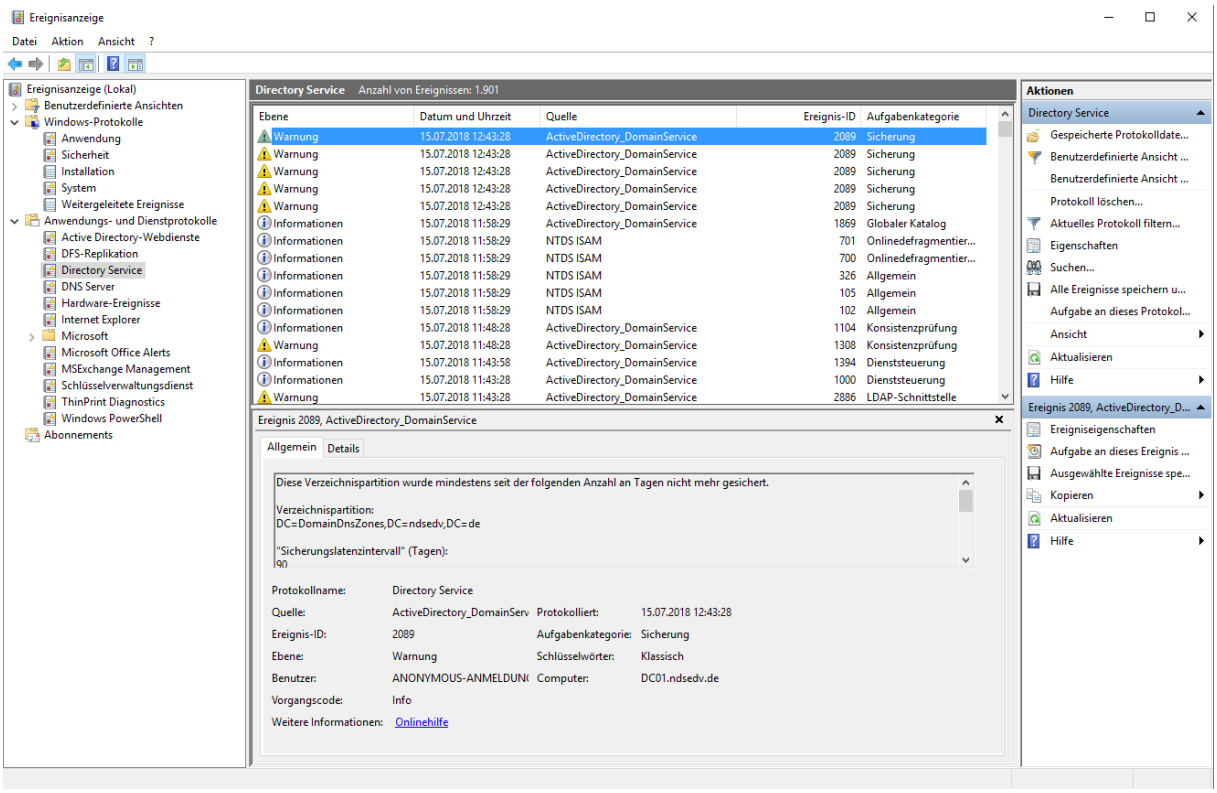
- Ereignis ID 1311
    - Probleme mit der Replikationstopologie. Die Replikationsinformationen im AD DS spiegeln nicht die physische Topologie wieder

Active Directory Health-Check

Check der Ereignisse in der DFS Replikation



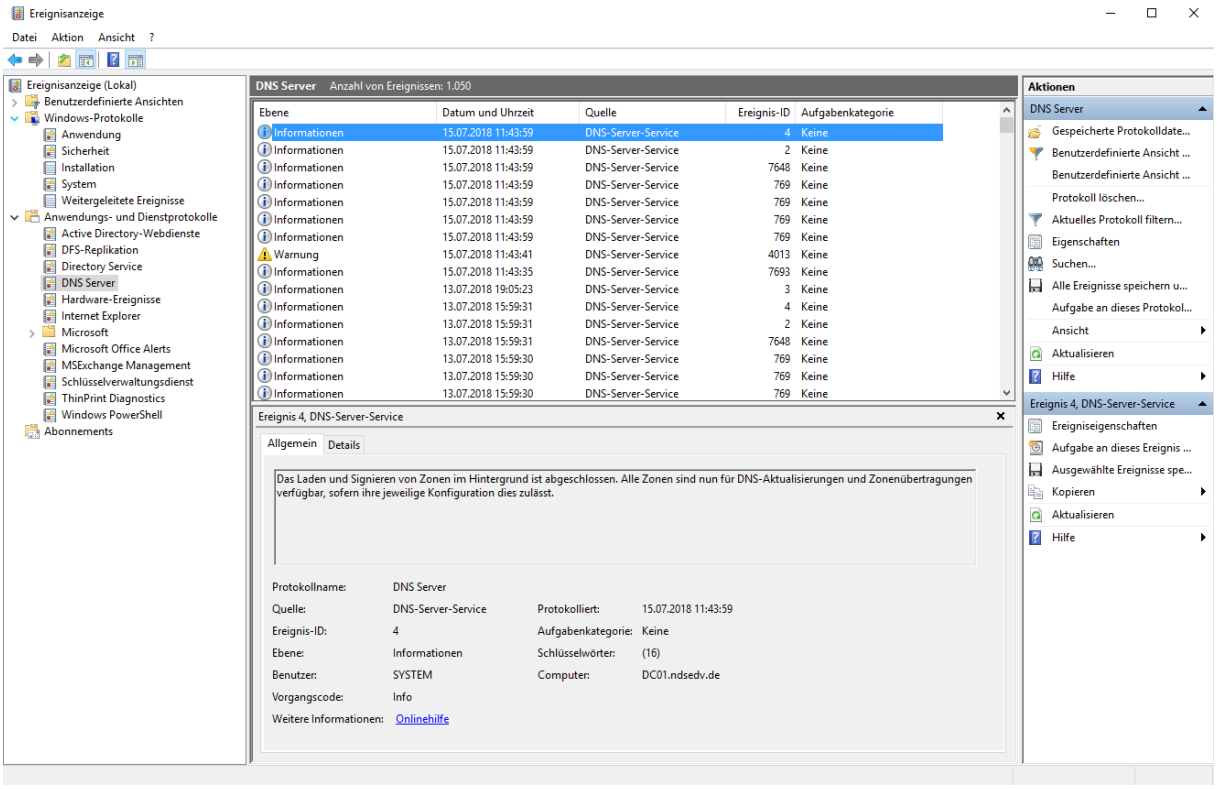
Check der Ereignisse in Directory Services



Erstellt von Jörn Walter **13.07.2018**

Active Directory Health-Check

Check der Ereignisse in DNS Server



https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc990288(v%3dws.10)

https://technet.microsoft.com/en-us/library/cc180912.aspx