



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



Active Directory Health-Check

- 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:

Server-Manager Dashboard

WILLKOMMEN BEI SERVER-MANAGER

- 1 Diesen lokalen Server konfigurieren
- 2 Rollen und Features hinzufügen
- 3 Weitere zu verwaltende Server hinzufügen
- 4 Servergruppe erstellen
- 5 Diesen Server mit Cloud-Diensten verbinden

Rollen und Servergruppen

Rollen: 4 | Servergruppen: 2 | Server insgesamt: 2

AD DS	Datei-/Speicherdienste	DHCP	DNS	DCs
2	2	1	2	2
Verwaltbarkeit	Verwaltbarkeit	Verwaltbarkeit	Verwaltbarkeit	Verwaltbarkeit
Ereignisse	Ereignisse	Ereignisse	Ereignisse	Ereignisse
Dienste	Dienste	Dienste	Dienste	Dienste
Leistung	Leistung	Leistung	Leistung	Leistung
BPA-Ergebnisse	BPA-Ergebnisse	BPA-Ergebnisse	BPA-Ergebnisse	BPA-Ergebnisse

13.07.2018 12:48

-Multiple Server

Server-Manager Alle Server

SERVER

Alle Server | 2 insgesamt

Servername	IPV4-Adresse	Verwaltbarkeit	Letztes Update	Windows-Aktivierung
DC01	172.18.32.31	Online - Leistungsindikatoren wurden nicht gestartet.	13.07.2018 12:48:50	00376-50575-66297-AA117 (Aktiviert)
DC02	172.18.32.32	Online - Leistungsindikatoren wurden nicht gestartet.	13.07.2018 12:49:16	Nicht aktiviert

EREIGNISSE

Alle Ereignisse | 70 insgesamt

Servername	ID	Schweregrad	Quelle	Protokoll	Datum und Uhrzeit
DC01	2006	Fehler	Microsoft-Windows-PerfNet	Anwendung	13.07.2018 12:48:49
DC01	2006	Fehler	Microsoft-Windows-PerfNet	Anwendung	13.07.2018 12:48:47
DC01	8233	Warnung	Microsoft-Windows-Security-SPP	Anwendung	13.07.2018 12:48:42
DC01	8233	Warnung	Microsoft-Windows-Security-SPP	Anwendung	13.07.2018 12:46:50
DC01	2006	Fehler	Microsoft-Windows-PerfNet	Anwendung	13.07.2018 12:46:45
DC01	12	Warnung	Microsoft-Windows-Time-Service	System	13.07.2018 12:46:41
DC01	10020	Warnung	Microsoft-Windows-DHCP-Server	System	13.07.2018 12:46:29

DIENTE

Alle Dienste | 211 insgesamt



Active Directory Health-Check

-Server Gruppen

Server-Manager Dashboard

WILLKOMMEN BEI SERVER-MANAGER

1 Diesen lokalen Server konfigurieren

2 Rollen und Servergruppen

3 Servergruppe erstellen

4 Servergruppe erstellen

5 Diesen Server mit Cloud-Diensten verbinden

Servergruppenname: DCs

Serverpool: Active Directory | DNS | Importieren

Name	IP-Adresse	Betriebssystem
DC02.ndsedv.de	172.18.32.32	Microsoft Windows Server 2012 R2
DC01.ndsedv.de	172.18.32.31	Microsoft Windows Server 2012 R2

Ausgewählt: Computer, NDSEDEV.DE (2)

2 Computer gefunden | 2 Computer ausgewählt

OK | Abbrechen

Rollen und Servergruppen

- AD DS (2)
- Verwaltbarkeit
- Ereignisse
- Dienste
- Leistung
- BPA-Ergebnisse

Alle Server (2)

Verwaltbarkeit

Lokaler Server (1)

- Verwaltbarkeit
- Ereignisse
- Dienste (3)
- Leistung
- BPA-Ergebnisse

13.07.2018 12:48

-Health Indikatoren

Server-Manager Dashboard

5 Diesen Server mit Cloud-Diensten verbinden

Rollen und Servergruppen

Rollen: 3 | Servergruppen: 2 | Server insgesamt: 1

- AD DS (1)
- Verwaltbarkeit
- Ereignisse
- Dienste
- Leistung
- BPA-Ergebnisse

- Datei-/Speicherdienste (1)
- Verwaltbarkeit
- Ereignisse
- Dienste
- Leistung
- BPA-Ergebnisse

- DNS (1)
- Verwaltbarkeit
- Ereignisse
- Dienste
- Leistung
- BPA-Ergebnisse

- DCs (1)
- Verwaltbarkeit
- Ereignisse
- Dienste (1)
- Leistung
- BPA-Ergebnisse

13.07.2018 13:06

- Lokaler Server (1)
- Verwaltbarkeit
- Ereignisse
- Dienste (1)
- Leistung
- BPA-Ergebnisse

13.07.2018 13:06

- Alle Server (1)
- Verwaltbarkeit
- Ereignisse
- Dienste (1)
- Leistung
- BPA-Ergebnisse

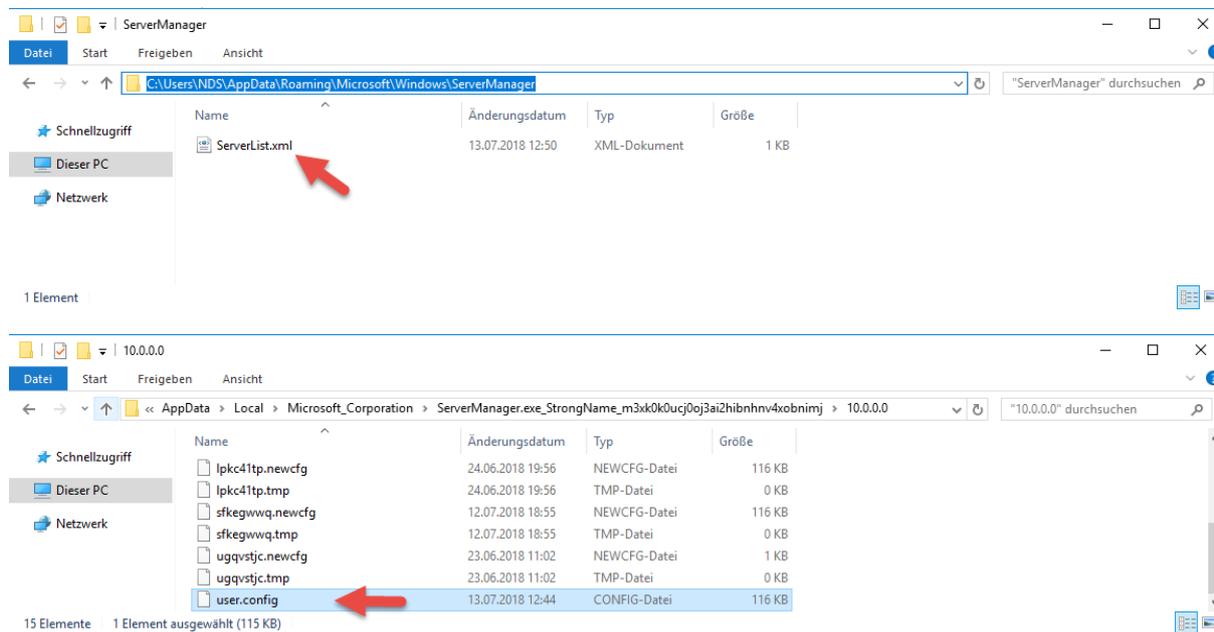
13.07.2018 13:06



Active Directory Health-Check

-Export/Import

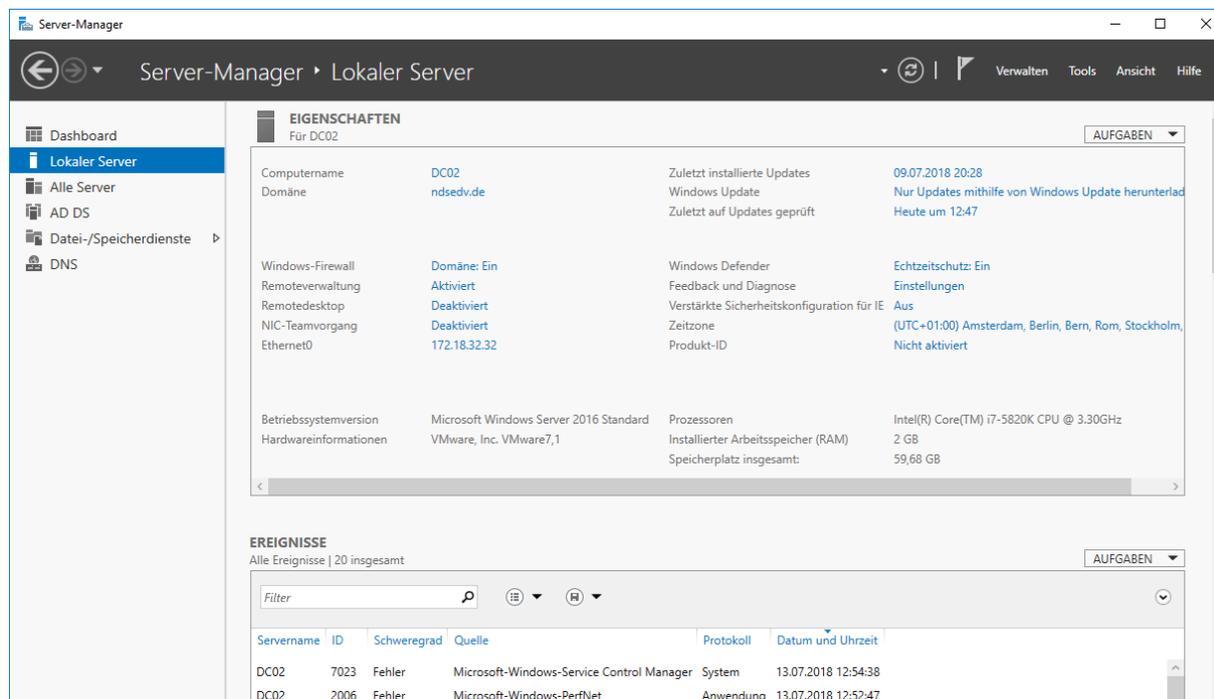
Export der Server Manager Einstellungen vom DC01:



-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

EIGENSCHAFTEN
Für DC02

Computername	DC02	Zuletzt installierte Updates	09.07.2018 20:28
Domäne	ndsebv.de	Windows Update	Nur Updates mithilfe von Windows Update herunterladen
		Zuletzt auf Updates geprüft	Heute um 12:47
Windows-Firewall	Domäne: Ein	Windows Defender	Echtzeitschutz: Ein
Remoteverwaltung	Aktiviert	Feedback und Diagnose	Einstellungen
Remotedesktop	Deaktiviert	Verstärkte Sicherheitskonfiguration für IE	Aus
NIC-Teamvorgang	Deaktiviert	Zeitzone	(UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
Ethernet0	172.18.32.32	Produkt-ID	Nicht aktiviert
Betriebssystemversion	Microsoft Windows Server 2016 Standard	Prozessoren	Intel(R) Core(TM) i7-5820K CPU @ 3.30GHz
Hardwareinformationen	VMware, Inc. VMware7,1	Installierter Arbeitsspeicher (RAM)	2 GB
		Speicherplatz insgesamt:	59,68 GB

EREIGNISSE
Alle Ereignisse | 23 insgesamt

Servername	ID	Schweregrad	Quelle	Protokoll	Datum und Uhrzeit
DC02	7023	Fehler	Microsoft-Windows-Service Control Manager	System	13.07.2018 12:59:38
DC02	7023	Fehler	Microsoft-Windows-Service Control Manager	System	13.07.2018 12:59:38
DC02	7023	Fehler	Microsoft-Windows-Service Control Manager	System	13.07.2018 12:59:38
DC02	7023	Fehler	Microsoft-Windows-Service Control Manager	System	13.07.2018 12:54:38
DC02	2006	Fehler	Microsoft-Windows-PerfNet	Anwendung	13.07.2018 12:52:47
DC02	2006	Fehler	Microsoft-Windows-PerfNet	Anwendung	13.07.2018 12:46:47

Events & Services

-Einzelansicht eines Servers

SERVER
Alle Server | 2 insgesamt

Servername	IPv4-Adresse	Verwaltbarkeit	Letztes Update	Windows-Aktivierung
DC01	172.18.32.31	Online - Leistungsindikatoren wurden nicht gestartet.	13.07.2018 13:14:42	00376-50575-66297-AA117 (Aktiviert)
DC02	172.18.32.32	Online - Leistungsindikatoren wurden nicht gestartet.	13.07.2018 13:14:50	Nicht aktiviert

EREIGNISSE
Alle Ereignisse | 72 insgesamt

Servername	ID	Schweregrad	Quelle	Protokoll	Datum und Uhrzeit
DC01	2006	Fehler	Microsoft-Windows-PerfNet	Anwendung	13.07.2018 12:54:47
DC01	10016	Fehler	Microsoft-Windows-DistributedCOM	System	13.07.2018 12:50:01
DC01	2006	Fehler	Microsoft-Windows-PerfNet	Anwendung	13.07.2018 12:48:49
DC01	2006	Fehler	Microsoft-Windows-PerfNet	Anwendung	13.07.2018 12:48:47
DC01	8233	Warnung	Microsoft-Windows-Security-SPP	Anwendung	13.07.2018 12:48:42
DC01	8233	Warnung	Microsoft-Windows-Security-SPP	Anwendung	13.07.2018 12:46:50
DC01	2006	Fehler	Microsoft-Windows-PerfNet	Anwendung	13.07.2018 12:46:45

DIENSTE
Alle Dienste | 211 insgesamt

Servername	Anzeigenname	Dienstname	Status	Starttyp
DC01	Automatische Konfiguration (verkabelt)	dot3svc	Beendet	Manuell
DC01	Diagnoserichtliniendienst	DPS	Wird ausgeführt	Automatisch (verzögerter Start)
DC01	DHCP-Client	Dhcp	Wird ausgeführt	Automatisch
DC01	Update Orchestrator Service für Windows Update	Usosvc	Beendet	Manuell



Active Directory Health-Check

-Gruppierte Ansicht zweier Server

SERVER
Alle Server | 2 insgesamt

Servername	IPv4-Adresse	Verwaltbarkeit	Letztes Update	Windows-Aktivierung
DC01	172.18.32.31	Online - Leistungsindikatoren wurden nicht gestartet.	13.07.2018 13:14:42	00376-50575-66297-AA117 (Aktiviert)
DC02	172.18.32.32	Online - Leistungsindikatoren wurden nicht gestartet.	13.07.2018 13:14:50	Nicht aktiviert

EREIGNISSE
Alle Ereignisse | 95 insgesamt

Servername	ID	Schweregrad	Quelle	Protokoll	Datum und Uhrzeit
DC02	7023	Fehler	Microsoft-Windows-Service Control Manager	System	13.07.2018 12:59:38
DC02	7023	Fehler	Microsoft-Windows-Service Control Manager	System	13.07.2018 12:59:38
DC02	7023	Fehler	Microsoft-Windows-Service Control Manager	System	13.07.2018 12:59:38
DC01	2006	Fehler	Microsoft-Windows-PerfNet	Anwendung	13.07.2018 12:54:47
DC02	7023	Fehler	Microsoft-Windows-Service Control Manager	System	13.07.2018 12:54:38
DC02	2006	Fehler	Microsoft-Windows-PerfNet	Anwendung	13.07.2018 12:52:47
DC01	10016	Fehler	Microsoft-Windows-DistributedCOM	System	13.07.2018 12:50:01

DIENSTE
Alle Dienste | 416 insgesamt

Servername	Anzeigename	Dienstname	Status	Starttyp
DC01	Automatische Konfiguration (verkabelt)	dot3svc	Beendet	Manuell
DC01	DHCP-Client	Dhcp	Wird ausgeführt	Automatisch
DC01	Update Orchestrator Service für Windows Update	Usosvc	Beendet	Manuell
DC01	Diagnosediensthost	WdiServiceHost	Beendet	Manuell

-Gefilterte Ansicht

SERVER
Alle Server | 2 insgesamt

Servername	IPv4-Adresse	Verwaltbarkeit	Letztes Update	Windows-Aktivierung
DC01	172.18.32.31	Online - Leistungsindikatoren wurden nicht gestartet.	13.07.2018 13:14:42	00376-50575-66297-AA117 (Aktiviert)
DC02	172.18.32.32	Online - Leistungsindikatoren wurden nicht gestartet.	13.07.2018 13:14:50	Nicht aktiviert

EREIGNISSE
Gefilterte Ergebnisse | 55 von 95 insgesamt

fehler

Servername	ID	Schweregrad	Quelle	Protokoll	Datum und Uhrzeit
DC02	7023	Fehler	Microsoft-Windows-Service Control Manager	System	13.07.2018 12:59:38
DC02	7023	Fehler	Microsoft-Windows-Service Control Manager	System	13.07.2018 12:59:38
DC02	7023	Fehler	Microsoft-Windows-Service Control Manager	System	13.07.2018 12:59:38
DC01	2006	Fehler	Microsoft-Windows-PerfNet	Anwendung	13.07.2018 12:54:47
DC02	7023	Fehler	Microsoft-Windows-Service Control Manager	System	13.07.2018 12:54:38

DIENSTE
Gefilterte Ergebnisse | 3 von 416 insgesamt

dhcp

Servername	Anzeigename	Dienstname	Status	Starttyp
DC01	DHCP-Client	Dhcp	Wird ausgeführt	Automatisch
DC01	DHCP-Server	DHCPsServer	Wird ausgeführt	Automatisch
DC02	DHCP-Client	Dhcp	Wird ausgeführt	Automatisch



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

Servername	Schweregrad	Titel	Kategorie
DC01	Warnung	DNS: Ethernet0 sollte sowohl für die Verwendung einer bevorzugten als auch eines alternativen DNS-Servers konfiguriert sein.	Konfiguration
DC01	Warnung	DNS: Stammhinweiserver 2001:503:c27:2:30 muss auf NS-Abfragen für die Stammzone reagieren.	Konfiguration
DC01	Warnung	DNS: Stammhinweiserver 2001:500:9f6:42 muss auf NS-Abfragen für die Stammzone reagieren.	Konfiguration
DC01	Warnung	DNS: Stammhinweiserver 2001:7fd:1 muss auf NS-Abfragen für die Stammzone reagieren.	Konfiguration
DC01	Warnung	DNS: Stammhinweiserver 2001:500:84:b muss auf NS-Abfragen für die Stammzone reagieren.	Konfiguration
DC01	Warnung	DNS: Stammhinweiserver 2001:500:2d:d muss auf NS-Abfragen für die Stammzone reagieren.	Konfiguration
DC01	Warnung	DNS: Stammhinweiserver 2001:500:2f:f muss auf NS-Abfragen für die Stammzone reagieren.	Konfiguration
DC01	Warnung	Alle Organisationseinheiten in der Domäne müssen vor versehentlichen Löschungen geschützt werden.	Konfiguration
DC01	Warnung	Die Verzeichnispartition CN=Configuration,DC=ndsenv,DC=de auf dem Domänencontroller DC01.ndsenv.de hätte innerhalb der letzten 8 Tage gesichert werden müssen.	Konfiguration
DC01	Warnung	Die Verzeichnispartition DC=ForestDnsZones,DC=ndsenv,DC=de auf dem Domänencontroller DC01.ndsenv.de hätte innerhalb der letzten 8 Tage gesichert werden müssen.	Konfiguration

-Probleme ermitteln

DC01 Warnung DHCP: Der Server muss über Vollzugriff auf die DHCP-Registrierungsparameter verfügen. Vor der Bereitstellung

Problem:
Der DHCP-Server verfügt nicht über Vollzugriff auf die DHCP-Registrierungsparameter.

Auswirkung:
Die Registrierungskonfiguration kann unter Umständen nicht gelesen und der DHCP-Server nicht gestartet werden.

[Weitere Informationen zu dieser bewährten Methode und den detaillierten Lösungsverfahren](#)



Active Directory Health-Check

-Lösungen

Für die ermittelten Probleme werden auch Lösungen angeboten.

Resolution

Assign the DHCPService service full control permissions to the DHCP registry.

To give DHCPService 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\DHCPService**.
3. Right-click **DHCPService** and then click **Permissions**.
4. In **Group or User names** click **DHCPService** if a DHCP Service is already present. Otherwise, click **Add** in **Select Users or Groups**.
5. Click **Locations** and select the hostname of the system, enter **NT Service\DHCPService**, and then, click **OK**.
6. In **Permissions for DHCP Service** check **Allow for Full control** and then click **OK**.

Performance:

-Leistungswarnungen

The screenshot shows the Windows Server Manager interface for a local server. The left-hand navigation pane includes options for Dashboard, Lokaler Server, Alle Server, AD DS, Datei-/Speicherdienste, DCs, DHCP, and DNS. The main area displays a 'LEISTUNG' (Performance) section with a graph for 'CPU-Auslastung' (CPU usage) over a 24-hour period. A red arrow points to the 'AUFGABEN' (Tasks) button in the top right of the performance section, which has opened a dropdown menu with options: 'Leistungswarnungen konfigurieren' (Configure performance warnings) and 'Aktualisieren' (Refresh). Below the graph, a table shows performance warnings for server DCO1:

Servername	Zählerstatus	Anzahl CPU-Warnungen	Anzahl Speicherwarnungen	Erstes Auftreten	Letztes Auftreten
DC01	Ein - Auf Daten wird gewartet	-	-	-	-

Below the performance section, the 'ROLLEN UND FEATURES' (Roles and Features) section is visible, showing a table with columns for Servername, Name, Typ, and Pfad. The first entry is DCO1, Active Directory-Domänendienste, Rolle, Active Directory-Domänendienste.



Active Directory Health-Check

-Speicher & CPU

The screenshot shows the Server-Manager interface for a local server. A dialog box titled "Lokaler Server : Leistungswarnungen konfigurieren" is open, allowing the user to set performance warning thresholds. The dialog contains the following information:

- Schwellenwerte für Leistungswarnungen festlegen**: Nachdem Sie Schwellenwerte geändert und auf "Speichern" geklickt haben, werden aktualisierte Daten für diese Gruppe oder Rolle angezeigt.
- CPU (% Auslastung)**: 5
- Arbeitsspeicher (verfügbare MB)**: 2
- Zeitraum der Leistungsdiagrammanzeige festlegen**: Im Leistungsdiagrammbereich für diese Rolle oder Servergruppe werden Leistungsdaten für die Anzahl von Tagen angezeigt, die in der Einstellung für den Zeitraum der Diagrammanzeige angegeben ist. Ein kleinerer Wert bewirkt, dass ein kürzeres Diagramm angezeigt wird.
- Zeitraum der Diagrammanzeige (Tage)**: 1

Buttons for "Speichern" and "Abbrechen" are visible at the bottom of the dialog.

Diagnose Tool – Performance Monitor:

-Echtzeitüberwachung

Die Leistungsüberwachung startet standardmäßig mit dem Indikator namens Prozessorzeit.

The screenshot shows the Performance Monitor (PerfMon) interface. The left pane shows the tree structure with "Leistung" expanded to "Leistung > Leistungsüberwachung". The main area displays a real-time graph of processor time. The graph shows a sharp spike in processor time around 14:45:25. Below the graph, the following statistics are displayed:

Statistik	Wert
Vorherige	1,205
Durchschnitt	1,620
Minimum	0,000
Maximum	62,495
Dauer	1:40

Below the statistics, the "Anzeigen" list is visible, showing the selected indicator "Prozessorzeit (%)" with a value of 1,0. The "Instanz" is set to "Total" and the "Objekt" is "Prozessorinformationen" on computer "\\DC01".

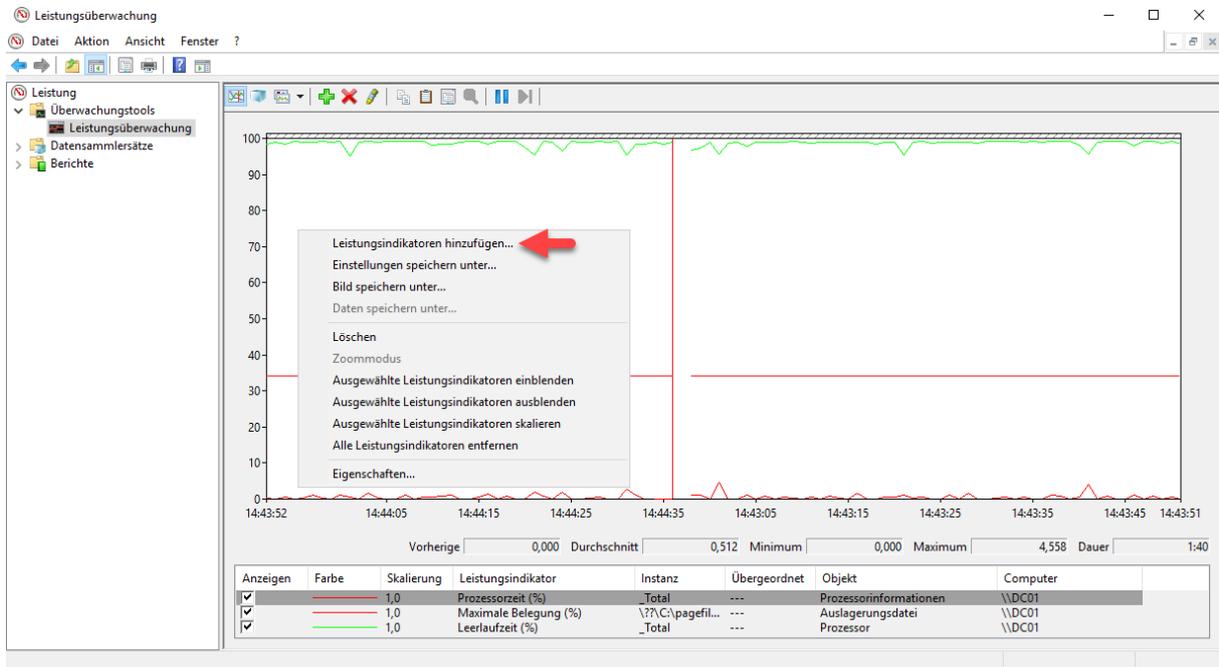


Active Directory Health-Check

Datensammlersätze

-Leistungsindikatoren

Weitere Indikatoren können über einen Rechtsklick zur Analyse hinzugefügt werden.



-Ereignisablaufverfolgung

Name	Status
AppModel	Wird ausgeführt
Audio	Wird ausgeführt
MSDTC_TRACE_SESSION	Wird ausgeführt
DiagLog	Wird ausgeführt
EventLog-AirSpaceChannel	Wird ausgeführt
EventLog-Application	Wird ausgeführt
EventLog-DebugChannel	Wird ausgeführt
EventLog-ForwardedEvents	Wird ausgeführt
EventLog-Microsoft-RMS-MSIPC-Debug	Wird ausgeführt
EventLog-System	Wird ausgeführt
NtfsLog	Wird ausgeführt
UAL_Usermode_Provider	Wird ausgeführt
UBPM	Wird ausgeführt
WdiContextLog	Wird ausgeführt
WindowsUpdate_trace_log	Wird ausgeführt
Diagtrack-Listener	Wird ausgeführt
MpWppTracing-20180713-155907-00000003-ffffff	Wird ausgeführt
UAL_Kernelmode_Provider	Wird ausgeführt



Active Directory Health-Check

-Systemkonfigurationsinformationen

Prüfung der Einträge in der Active Directory Registry

Name	Typ	Ausgabe
NT Kernel	Ablaufverfolgung	C:\perflogs\ADDS\20180713-0001\NtKernel.etl
Active Directory	Ablaufverfolgung	C:\perflogs\ADDS\20180713-0001\Active Directory.etl
Performance Counter	Leistungsindikatoren	C:\perflogs\ADDS\20180713-0001\Performance.Counter.big
AD Registry	Konfiguration	C:\perflogs\ADDS\20180713-0001\AD Registry.xml

Eigenschaften von AD Registry

Registrierungsschlüssel:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Wdpp...
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Wdsc...
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Wdt...
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WTD...
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip...
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip...
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip...
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip...
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip...

Prüfung des gesamten Systems

Name	Typ	Ausgabe
NT Kernel	Ablaufverfolgung	C:\perflogs\System\Diagnosics\DC02_20180713-000001\NtKernel.etl
Operating System	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Operating System.xml
Processor	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Processor.xml
System Services	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\System Services.xml
Logical Disk Dirty Test	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Logical Disk Dirty Test.xml
SMART Disk Check	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\SMART Disk Check.xml
AntiSpywareProduct	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\AntiSpywareProduct.xml
FirewallProduct	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\FirewallProduct.xml
AntiVirusProduct	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\AntiVirusProduct.xml
UAC Settings	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\UAC Settings.xml
Windows Update Settings	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Windows Update Settings.xml
Performance Counter	Leistungsindikatoren	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Performance.Counter.big
BIOS	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\BIOS.xml
Controller Classes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Controller Classes.xml
Cooling Classes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Cooling Classes.xml
Input Classes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Input Classes.xml
Memory Classes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Memory Classes.xml
Motherboard Classes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Motherboard Classes.xml
Network Classes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Network Classes.xml
Port Classes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Port Classes.xml
PlugAndPlay Classes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\PlugAndPlay Classes.xml
Power Classes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Power Classes.xml
Printing Classes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Printing Classes.xml
Storage Classes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Storage Classes.xml
Video Classes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Video Classes.xml
NTFS Performance	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\NTFS Performance.xml
Interactive Session Processes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Interactive Session Processes.xml
Interactive Sessions	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Interactive Sessions.xml
Processes	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Processes.xml
Logged On Users	Konfiguration	C:\perflogs\System\Diagnosics\DC02_20180713-000001\Logged On Users.xml



Active Directory Health-Check

Prüfung der Systemperformance

Name	Typ	Ausgabe
NT Kernel	Ablaufverfolgung	
Performance Counter	Leistungsindikatoren	

Eigenschaften von System Performance (Systemleistung)

Name: System Performance

Beschreibung: Generiert einen Bericht, der detaillierte Informationen zum Status der lokalen Hardwareressourcen, den Systemantwortzeiten und den Prozessen auf dem lokalen Computer enthält. Anhand dieser Informationen können Sie mögliche Ursachen von Leistungsproblemen

Schlüsselwörter: CPU, Memory, Disk, Network, Performance

Ausführen als:

Buttons: OK, Abbrechen, Übernehmen

-Systemkonfigurationsinformations-Bericht

Warnung: Die Datenträger-Bewertung für das System ist unzureichend und kann die Ursache der Leistungsprobleme sein. Schließen Sie einige der offenen Anwendungen, Dadurch wird die Systemleistung möglicherweise verbessert. Stellen Sie sicher, dass der Datenträger über ausreichend freien Speicherplatz verfügt und defragmentiert ist. Überprüfen Sie die Autostartanwendungen, und deaktivieren Sie die Autostartanwendungen, die Sie nicht benötigen. Wenn das Problem weiterhin besteht, muss der Datenträger möglicherweise durch einen neuen ersetzt werden.

Verwandt: [Leistungsdiagnose](#)

Schweregrad: Informationen

Warnung: Die Arbeitsspeicher-Bewertung für das System ist unzureichend und kann die Ursache der Leistungsprobleme sein. Schließen Sie einige der offenen Anwendungen, Dadurch wird die Systemleistung möglicherweise verbessert. Überprüfen Sie die Autostartanwendungen, und deaktivieren Sie die Autostartanwendungen, die Sie nicht benötigen. Wenn das Problem weiterhin besteht, muss der Arbeitsspeicher möglicherweise erweitert werden.

Verwandt: [Leistungsdiagnose](#)

Grundlegende Systemprüfungen

Tests	Ergebnis	Beschreibung
Betriebssystemprüfungen	Durchgeführt	Überprüft die Attribute des Betriebssystems.
Datenträgerprüfungen	Durchgeführt	Überprüft den Datenträgerstatus.
Sicherheitscenter-Tests	Durchgeführt	Überprüft den Status der Informationen, die sich auf das Sicherheitscenter beziehen.
Systemdienstprüfungen	Durchgeführt	Überprüft den Status der Systemdienste.
Hardwaregeräte- und Treiberprüfungen	Durchgeführt	Überblick über die von der Windows-Verwaltungsinfrastruktur unterstützten Geräte.

Leistung

Ressourcenübersicht

Komponente	Status	Verwendung	Details
CPU	Im Leerlauf	7 %	Geringe CPU-Belastung.
Netzwerk	Im Leerlauf	0 %	Der Netzwerkkadpter mit der höchsten Auslastung liegt unter 15%.
Datenträger	Normal	109 /sec	Die Datenträger-E/A's liegen zwischen 100 und 500 Vorgängen (Lesen/Schreiben) pro Sekunde auf dem Datenträger 0.
Arbeitsspeicher	Normal	65 %	712 MB verfügbar.

Softwarekonfiguration

Hardwarekonfiguration

CPU

Fertig



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.

The screenshot shows the Windows Performance Monitor (Leistung) tool. The left pane displays a tree view of monitoring tools, with 'Active Directory Diagnostics' selected under 'System'. The right pane shows the 'Systemleistungsbericht' (System Performance Report) for computer DC02, collected on Friday, July 13, 2018, at 16:38:26, with a duration of 5 seconds.

Zusammenfassung

Verarbeiten	Datenträger	Arbeitsspeicher	Netzwerk
CPU % insgesamt: 2	Top-Datenträger nach E/A-Rate: 0	Verwendung: 58 %	Verwendung: 0 %
Obere Prozessgruppe: mmc.exe	EA/s: 9	Arbeitsspeicher: 2047 MB	Beste ausgehende Client: 127.0.0.1
Gruppen-CPU %: 2	Länge der Datenträgerwarteschlange: 0.004	Oberer Prozess: dns	Gesendet: 622 Bytes
CPU % insgesamt: 0		Privater Arbeitssatz: 61,204 KB	Beste eingehende Client: 127.0.0.1
Obere Prozessgruppe:			Empfangen: 622 Bytes

Diagnoseergebnisse

Leistung

Ressourcenübersicht

Komponente	Status	Verwendung	Details
CPU	Im Leerlauf	6 %	Geringe CPU-Belastung.
Netzwerk	Im Leerlauf	0 %	Der Netzwerkkappter mit der höchsten Auslastung liegt unter 15%.
Datenträger	Im Leerlauf	9/sec	Die Datenträger-E/As betragen weniger als 100 Vorgänge (Lesen/Schreiben) pro Sekunde auf dem Datenträger 0.
Arbeitsspeicher	Normal	58 %	867 MB verfügbar.

The bottom of the window shows expandable sections for CPU, Netzwerk, Datenträger, and Arbeitsspeicher.

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.ndsdev.de is the RID Master
* DsBind with RID Master was successful
rIDSetReferences = CN=RID Set,CN=DC01,OU=Domain Controllers,DC=ndsdev,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=ndsdev,DC=de sowie der Backlink auf
CN=DC01,CN=Servers,CN=Essen,CN=Sites,CN=Configuration,DC=ndsdev,DC=de sind korrekt.
Der Systemobjektverweis (serverReferenceBL)
CN=DC01,CN=Topology,CN=Domain System Volume,CN=DFSR-GlobalSettings,CN=System,DC=ndsdev,DC=de sowie der
Backlink auf CN=NTDS Settings,CN=DC01,CN=Servers,CN=Essen,CN=Sites,CN=Configuration,DC=ndsdev,DC=de sind
korrekt.
Der Systemobjektverweis (msDFSR-ComputerReferenceBL)
CN=DC01,CN=Topology,CN=Domain System Volume,CN=DFSR-GlobalSettings,CN=System,DC=ndsdev,DC=de sowie der
Backlink auf CN=DC01,OU=Domain Controllers,DC=ndsdev,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 ausgeführt auf: DomainDnsZones
Starting test: CheckSDRefDom
```



Active Directory Health-Check

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

```
Administrator: Eingabeaufforderung
C:\Windows\system32>dcdiag /test:dns /dnsbasic
Verzeichnisserverdiagnose
Anfangssetup wird ausgeführt:
  Der Homeserver wird gesucht...
  Homeserver = DC01
  * Identifizierte AD-Gesamtstruktur.
  Sammeln der Ausgangsinformationen abgeschlossen.
Erforderliche Anfangstests werden ausgeführt.
  Server wird getestet: Essen\DC01
  Starting test: Connectivity
  ..... DC01 hat den Test Connectivity bestanden.
Primärtests werden ausgeführt.
  Server wird getestet: Essen\DC01
  Starting test: DNS
  DNS-Tests werden ordnungsgemäß ausgeführt. Warten Sie einige Minuten...
  ..... DC01 hat den Test DNS bestanden.
Partitionstests werden ausgeführt auf: DomainDnsZones
Partitionstests werden ausgeführt auf: ForestDnsZones
Partitionstests werden ausgeführt auf: Schema
Partitionstests werden ausgeführt auf: Configuration
Partitionstests werden ausgeführt auf: ndsedv
Unternehmenstests werden ausgeführt auf: ndsedv.de
Starting test: DNS
..... ndsedv.de hat den Test DNS bestanden.
C:\Windows\system32>
```

- DCdiag /test:dns /dnsall

```
Administrator: Eingabeaufforderung
C:\Windows\system32>dcdiag /test:dns /dnsall
Verzeichnisserverdiagnose
Anfangssetup wird ausgeführt:
  Der Homeserver wird gesucht...
  Homeserver = DC01
  * Identifizierte AD-Gesamtstruktur.
  Sammeln der Ausgangsinformationen abgeschlossen.
Erforderliche Anfangstests werden ausgeführt.
  Server wird getestet: Essen\DC01
  Starting test: Connectivity
  ..... DC01 hat den Test Connectivity bestanden.
Primärtests werden ausgeführt.
  Server wird getestet: Essen\DC01
  Starting test: DNS
  DNS-Tests werden ordnungsgemäß ausgeführt. Warten Sie einige Minuten...
  ..... DC01 hat den Test DNS bestanden.
Partitionstests werden ausgeführt auf: DomainDnsZones
Partitionstests werden ausgeführt auf: ForestDnsZones
Partitionstests werden ausgeführt auf: Schema
Partitionstests werden ausgeführt auf: Configuration
Partitionstests werden ausgeführt auf: ndsedv
Unternehmenstests werden ausgeführt auf: ndsedv.de
Starting test: DNS
..... ndsedv.de hat den Test DNS bestanden.
C:\Windows\system32>
```

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

```
Administrator: Eingabeaufforderung
Primärtests werden ausgeführt.

Server wird getestet: Essen\DC01
Starting test: Advertising
  The DC DC01 is advertising itself as a DC and having a DS.
  The DC DC01 is advertising as an LDAP server
  The DC DC01 is advertising as having a writeable directory
  The DC DC01 is advertising as a Key Distribution Center
  The DC DC01 is advertising as a time server
  The DS DC01 is advertising as a GC.
..... DC01 hat den Test Advertising bestanden.
Starting test: CheckSecurityError
* Dr Auth: Beginning security errors check!
Found KDC DC01 for domain ndsedv.de in site Essen
Checking machine account for DC DC01 on DC DC01.
* SPN found :LDAP/DC01.ndsedv.de/ndsedv.de
* SPN found :LDAP/DC01.ndsedv.de
* SPN found :LDAP/DC01
* SPN found :LDAP/DC01.ndsedv.de/NDSSESV
* SPN found :LDAP/70c5c51a-6066-4445-8803-97e2f51dd661._msdcs.ndsedv.de
* SPN found :E3514235-4B06-11D1-AB04-00C04FC2DCD2/70c5c51a-6066-4445-8803-97e2f51dd661/ndsedv.de
* SPN found :HOST/DC01.ndsedv.de/ndsedv.de
* SPN found :HOST/DC01.ndsedv.de
* SPN found :HOST/DC01
* SPN found :HOST/DC01.ndsedv.de/NDSSESV
* SPN found :GC/DC01.ndsedv.de/ndsedv.de
[DC01] Auf dem Domänencontroller wurden keine sicherheitsbedingten Replikationsfehler gefunden. Verwenden Sie
den folgenden Befehl, um die Verbindung an einen bestimmten Quelldomänencontroller zu richten:
/ReplSource:<Domänencontroller>.
..... DC01 hat den Test CheckSecurityError bestanden.
Starting test: CutoffServers
* Configuration Topology Aliveness Check
* Analyzing the alive system replication topology for DC=DomainDnsZones,DC=ndsedv,DC=de.
* Performing upstream (of target) analysis.
* Performing downstream (of target) analysis.
* Analyzing the alive system replication topology for DC=ForestDnsZones,DC=ndsedv,DC=de.
* Performing upstream (of target) analysis.
* Performing downstream (of target) analysis.
* Analyzing the alive system replication topology for CN=Schema,CN=Configuration,DC=ndsedv,DC=de.
* Performing upstream (of target) analysis.
* Performing downstream (of target) analysis.
* Analyzing the alive system replication topology for CN=Configuration,DC=ndsedv,DC=de.
* Performing upstream (of target) analysis.
* Performing downstream (of target) analysis.
```



Active Directory Health-Check

Diagnose Tool – Repadmin:

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

Zeigt eine Zusammenfassung

```
Administrator: Eingabeaufforderung
C:\Windows\system32>repadmin /replsummary
Startzeit der Replikationszusammenfassung: 2018-07-13 18:39:38

Datensammlung für Replikationszusammenfassung wird gestartet.
Dieser Vorgang kann einige Zeit dauern.
.....

Quell-DSA          Größtes Delta   Fehler/gesamt  %% Fehler
DC01               47m:56s        0 / 5         0
DC02               40m:38s        0 / 5         0

Ziel-DSA           Größtes Delta   Fehler/gesamt  %% Fehler
DC01               40m:38s        0 / 5         0
DC02               47m:56s        0 / 5         0

C:\Windows\system32>
```

Zeigt die Objekte an

```
Administrator: Eingabeaufforderung
C:\Windows\system32>repadmin /showrepl

Repadmin: Befehl "/showrepl" wird für den vollständigen DC "localhost" ausgeführt
Essen\DC01
DSA-Optionen: IS_GC
Standortoptionen: (none)
DSA-Objekt-GUID: 70c5c51a-6066-4445-8803-97e2f51dd661
DSA-Aufrufkennung: 70c5c51a-6066-4445-8803-97e2f51dd661

==== EINGEHENDE NACHBARN====

DC=ndsedv,DC=de
  Essen\DC02 über RPC
  DSA-Objekt-GUID: 681de32b-44e5-412c-8460-7649a98a79b7
  Letzter Versuch am 2018-07-13 17:59:00 war erfolgreich.

CN=Configuration,DC=ndsedv,DC=de
  Essen\DC02 über RPC
  DSA-Objekt-GUID: 681de32b-44e5-412c-8460-7649a98a79b7
  Letzter Versuch am 2018-07-13 17:59:00 war erfolgreich.

CN=Schema,CN=Configuration,DC=ndsedv,DC=de
  Essen\DC02 über RPC
  DSA-Objekt-GUID: 681de32b-44e5-412c-8460-7649a98a79b7
  Letzter Versuch am 2018-07-13 17:59:00 war erfolgreich.

DC=ForestDnsZones,DC=ndsedv,DC=de
  Essen\DC02 über RPC
  DSA-Objekt-GUID: 681de32b-44e5-412c-8460-7649a98a79b7
  Letzter Versuch am 2018-07-13 17:59:00 war erfolgreich.

DC=DomainDnsZones,DC=ndsedv,DC=de
  Essen\DC02 über RPC
  DSA-Objekt-GUID: 681de32b-44e5-412c-8460-7649a98a79b7
  Letzter Versuch am 2018-07-13 18:28:50 war erfolgreich.

C:\Windows\system32>
```



Active Directory Health-Check

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)

```
Administrator: Eingabeaufforderung
C:\Windows\system32>repadmin /syncall /e
RÜCKRUFMELDUNG: Die folgende Replikation wird ausgeführt:
  Von: 681de32b-44e5-412c-8460-7649a98a79b7._msdcs.ndsedv.de
  An : 70c5c51a-6066-4445-8803-97e2f51dd661._msdcs.ndsedv.de
RÜCKRUFMELDUNG: Die folgende Replikation wurde erfolgreich abgeschlossen:
  Von: 681de32b-44e5-412c-8460-7649a98a79b7._msdcs.ndsedv.de
  An : 70c5c51a-6066-4445-8803-97e2f51dd661._msdcs.ndsedv.de
RÜCKRUFMELDUNG: SyncAll wurde abgeschlossen.
SyncAll wurde ohne Fehler beendet.

C:\Windows\system32>repadmin /syncall /aped
RÜCKRUFMELDUNG: Die folgende Replikation wird ausgeführt:
  Von: CN=NTDS Settings,CN=DC02,CN=Servers,CN=Essen,CN=Sites,CN=Configuration,DC=ndsedv,DC=de
  An : CN=NTDS Settings,CN=DC01,CN=Servers,CN=Essen,CN=Sites,CN=Configuration,DC=ndsedv,DC=de
Beenden mit Q, Fortsetzen mit beliebiger Taste.
RÜCKRUFMELDUNG: Die folgende Replikation wurde erfolgreich abgeschlossen:
  Von: CN=NTDS Settings,CN=DC02,CN=Servers,CN=Essen,CN=Sites,CN=Configuration,DC=ndsedv,DC=de
  An : CN=NTDS Settings,CN=DC01,CN=Servers,CN=Essen,CN=Sites,CN=Configuration,DC=ndsedv,DC=de
Beenden mit Q, Fortsetzen mit beliebiger Taste.
RÜCKRUFMELDUNG: SyncAll wurde abgeschlossen.
SyncAll wurde ohne Fehler beendet.

C:\Windows\system32>_
```

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

```
Administrator: Eingabeaufforderung
C:\Windows\system32>repadmin /kcc *
Repadmin: Befehl "/kcc" wird für den vollständigen DC "DC01.ndsedv.de" ausgeführt
Essen
Aktuell Standortoptionen: (none)
Die Konsistenzüberprüfung auf DC01.ndsedv.de war erfolgreich.

Repadmin: Befehl "/kcc" wird für den vollständigen DC "DC02.ndsedv.de" ausgeführt
Essen
Aktuell Standortoptionen: (none)
Die Konsistenzüberprüfung auf DC02.ndsedv.de war erfolgreich.

C:\Windows\system32>
```



Active Directory Health-Check

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

```
Administrator: Eingabeaufforderung

C:\Windows\system32>repadmin /showbackup *

Repadmin: Befehl "/showbackup" wird für den vollständigen DC "DC01.ndserved.de" ausgeführt

Lok.USN                Ursprüngl. DSA        Ur. USN  Ur.Zeit/Datum        Ver Attribut
=====                =
DC=DomainDnsZones,DC=ndserved,DC=de
13055      70c5c51a-6066-4445-8803-97e2f51dd661    13055  2016-11-19 16:53:01    1 dSASignature
DC=ForestDnsZones,DC=ndserved,DC=de
13054      70c5c51a-6066-4445-8803-97e2f51dd661    13054  2016-11-19 16:53:01    1 dSASignature
CN=Schema,CN=Configuration,DC=ndserved,DC=de
13053      70c5c51a-6066-4445-8803-97e2f51dd661    13053  2016-11-19 16:53:01    1 dSASignature
CN=Configuration,DC=ndserved,DC=de
13052      70c5c51a-6066-4445-8803-97e2f51dd661    13052  2016-11-19 16:53:01    1 dSASignature
DC=ndserved,DC=de
13051      70c5c51a-6066-4445-8803-97e2f51dd661    13051  2016-11-19 16:53:01    1 dSASignature

Repadmin: Befehl "/showbackup" wird für den vollständigen DC "DC02.ndserved.de" ausgeführt

Lok.USN                Ursprüngl. DSA        Ur. USN  Ur.Zeit/Datum        Ver Attribut
=====                =
DC=DomainDnsZones,DC=ndserved,DC=de
16873      70c5c51a-6066-4445-8803-97e2f51dd661    13055  2016-11-19 16:53:01    1 dSASignature
DC=ForestDnsZones,DC=ndserved,DC=de
16835      70c5c51a-6066-4445-8803-97e2f51dd661    13054  2016-11-19 16:53:01    1 dSASignature
CN=Schema,CN=Configuration,DC=ndserved,DC=de
4101      70c5c51a-6066-4445-8803-97e2f51dd661    13053  2016-11-19 16:53:01    1 dSASignature
CN=Configuration,DC=ndserved,DC=de
9209      70c5c51a-6066-4445-8803-97e2f51dd661    13052  2016-11-19 16:53:01    1 dSASignature
DC=ndserved,DC=de
14105      70c5c51a-6066-4445-8803-97e2f51dd661    13051  2016-11-19 16:53:01    1 dSASignature

C:\Windows\system32>
```

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

```
Administrator: Eingabeaufforderung

C:\Windows\system32>repadmin /showoutcalls *

Repadmin: Befehl "/showoutcalls" wird für den vollständigen DC "DC01.ndserved.de" ausgeführt
DC01.ndserved.de versucht, zurzeit keine ausgehenden DRS-RPC-Aufrufe durchzuführen.

Repadmin: Befehl "/showoutcalls" wird für den vollständigen DC "DC02.ndserved.de" ausgeführt
DC02.ndserved.de versucht, zurzeit keine ausgehenden DRS-RPC-Aufrufe durchzuführen.

C:\Windows\system32>
```



Active Directory Health-Check

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

```
Administrator: Eingabeaufforderung
C:\Windows\system32>repadmin /bridgeheads * /verbose
Repadmin: Befehl "/bridgeheads" wird für den vollständigen DC "DC01.ndsedv.de" ausgeführt
Topologie von Standort Essen (DC01.ndsedv.de) wird zusammengestellt:
Bridgeheads für Standort Essen (DC01.ndsedv.de):
  Quellstandort   Lokale Brücke   Trns   Fehlerzeit   Nr.   Status
  =====
Bridgeheads für Standort Essen (DC01.ndsedv.de):
  Quellstandort   Lokale Brücke   Trns   Fehlerzeit   Nr.   Status
  =====
Repadmin: Befehl "/bridgeheads" wird für den vollständigen DC "DC02.ndsedv.de" ausgeführt
Topologie von Standort Essen (DC02.ndsedv.de) wird zusammengestellt:
Bridgeheads für Standort Essen (DC01.ndsedv.de):
  Quellstandort   Lokale Brücke   Trns   Fehlerzeit   Nr.   Status
  =====
Bridgeheads für Standort Essen (DC01.ndsedv.de):
  Quellstandort   Lokale Brücke   Trns   Fehlerzeit   Nr.   Status
  =====
C:\Windows\system32>
```

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

```
Auswählen Administrator: Eingabeaufforderung
C:\Windows\system32>repadmin /istg * /verbose
Repadmin: Befehl "/istg" wird für den vollständigen DC "DC01.ndsedv.de" ausgeführt
Topologie von Standort Essen (DC01.ndsedv.de) wird zusammengestellt:
  Standort   ISTG
  =====
Default-First-Site-Name   DC01
  Essen                   DC01
Repadmin: Befehl "/istg" wird für den vollständigen DC "DC02.ndsedv.de" ausgeführt
Topologie von Standort Essen (DC02.ndsedv.de) wird zusammengestellt:
  Standort   ISTG
  =====
Default-First-Site-Name   DC01
  Essen                   DC01
C:\Windows\system32>
```



Active Directory Health-Check

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

```
Administrator: Eingabeaufforderung
C:\Windows\system32>repadmin /failcache *
Repadmin: Befehl "/failcache" wird für den vollständigen DC "DC01.ndsedv.de" ausgeführt
==== KCC-VERBINDUNGSFEHLER =====
(keine)

==== KCC-VERKNÜPFUNGSFEHLER =====
Essen\DC02
DSA-Objekt-GUID: 681de32b-44e5-412c-8460-7649a98a79b7
Keine Fehler.

Repadmin: Befehl "/failcache" wird für den vollständigen DC "DC02.ndsedv.de" ausgeführt
==== KCC-VERBINDUNGSFEHLER =====
(keine)

==== KCC-VERKNÜPFUNGSFEHLER =====
(keine)

C:\Windows\system32>
```

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

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. Alle Rechte vorbehalten.
C:\Windows\system32>Repadmin /showtrust *
Repadmin: Befehl "/showtrust" wird für den vollständigen DC "DC01.ndsedv.de" ausgeführt
Domänenvertrauensinformationen:
VERTRAUT      : DC=ndsedv,DC=de

Repadmin: Befehl "/showtrust" wird für den vollständigen DC "DC02.ndsedv.de" ausgeführt
Domänenvertrauensinformationen:
VERTRAUT      : DC=ndsedv,DC=de

C:\Windows\system32>_
```



Active Directory Health-Check

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

```
Administrator: Eingabeaufforderung
C:\Windows\system32>repadmin /bind *

Repadmin: Befehl "/bind" wird für den vollständigen DC "DC01.ndsedv.de" ausgeführt
Bindung an DC01.ndsedv.de war erfolgreich.
NTDSAPI V1 BindState, erweiterte Mitglieder werden gedruckt.
  bindAddr: DC01.ndsedv.de
Unterstützte Erweiterungen (cb=52):
  BASE : Ja
  ASYNCREPL : Ja
  REMOVEAPI : Ja
  MOVEREQ_V2 : Ja
  GETCHG_COMPRESS : Ja
  DCINFO_V1 : Ja
  RESTORE_USN_OPTIMIZATION : Ja
  KCC_EXECUTE : Ja
  ADDENTRY_V2 : Ja
  LINKED_VALUE_REPLICATION : Ja
  DCINFO_V2 : Ja
  INSTANCE_TYPE_NOT_REQ_ON_MOD : Ja
  CRYPTO_BIND : Ja
  GET_REPL_INFO : Ja
  STRONG_ENCRYPTION : Ja
  DCINFO_VFFFFFFFF : Ja
  TRANSITIVE_MEMBERSHIP : Ja
  ADD_SID_HISTORY : Ja
  POST_BETA3 : Ja
  GET_MEMBERSHIPS2 : Ja
  GETCHGREQ_V6 (WINDOWS XP PREVIEW): Ja
  NONDOMAIN_NCS : Ja
  GETCHGREQ_V8 (WINDOWS XP BETA 1) : Ja
  GETCHGREPLY_V5 (WINDOWS XP BETA 2): Ja
  GETCHGREPLY_V6 (WINDOWS XP BETA 2): Ja
  ADDENTRYREPLY_V3 (WINDOWS XP BETA 3): Ja
  GETCHGREPLY_V7 (WINDOWS XP BETA 3) : Ja
  VERIFY_OBJECT (WINDOWS XP BETA 3): Ja
  XPRESS_COMPRESSION : Ja
  DRS_EXT_ADAM : Nein
  GETCHGREQ_V10 : Ja
  RECYCLE_BIN_FEATURE : Nein
Standort-GUID: 74d15933-c9e3-486d-aea6-b9f24528c37d
Replikationsepoche: 0
Gesamtstruktur-GUID: c7081dc7-d7c1-4d5f-9cc7-414c322169eb
Die Sicherungsinformationen auf der Bindung sind wie folgt:
Angeforderter SPN: LDAP/DC01.ndsedv.de
Authentifizierungsdienst: 9
```

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

Event Viewer (Ereignisanzeige) - DFS-Replikation (Anzahl von Ereignissen: 515)

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	15.07.2018 11:49:00	DFSR	5004	Keine
Fehler	15.07.2018 11:48:57	DFSR	5002	Keine
Informationen	15.07.2018 11:48:50	DFSR	1210	Keine
Informationen	15.07.2018 11:48:50	DFSR	1206	Keine
Fehler	15.07.2018 11:43:49	DFSR	1202	Keine
Informationen	15.07.2018 11:43:37	DFSR	6102	Keine
Informationen	15.07.2018 11:43:36	DFSR	1314	Keine
Informationen	15.07.2018 11:43:35	DFSR	1004	Keine
Informationen	15.07.2018 11:43:35	DFSR	1002	Keine
Informationen	13.07.2018 16:21:50	DFSR	5004	Keine
Fehler	13.07.2018 16:14:54	DFSR	5008	Keine
Fehler	13.07.2018 16:07:16	DFSR	5008	Keine
Informationen	13.07.2018 16:04:21	DFSR	1210	Keine
Informationen	13.07.2018 16:04:21	DFSR	1206	Keine
Fehler	13.07.2018 15:59:21	DFSR	1202	Keine
Informationen	13.07.2018 15:59:09	DFSR	6102	Keine

Ereignis 5004, DFSR

Allgemein Details

Der DFS-Replikationsdienst hat erfolgreich eine eingehende Verbindung mit Partner "DC02" für Replikationsgruppe "Domain System Volume" hergestellt.

Weitere Informationen:
Verwendete Verbindungsadresse: DC02.ndsedv.de
Verbindungs-ID: C64EB68C-F124-413A-BD89-ED7690473BF3
Replikationsgruppen-ID: C57D8RE63-47C4-4944-R776-80796F3D4D77

Protokollname: DFS-Replikation
Quelle: DFSR Protokolliert: 15.07.2018 11:49:00
Ereignis-ID: 5004 Aufgabenkategorie: Keine
Ebene: Informationen Schlüsselwörter: Klassisch
Benutzer: Nicht zutreffend Computer: DC01.ndsedv.de
Vorgangscod:
Weitere Informationen: [Onlinehilfe](#)

Check der Ereignisse in Directory Services

Event Viewer (Ereignisanzeige) - Directory Service (Anzahl von Ereignissen: 1.901)

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Warnung	15.07.2018 12:43:28	ActiveDirectory_DomainService	2089	Sicherung
Warnung	15.07.2018 12:43:28	ActiveDirectory_DomainService	2089	Sicherung
Warnung	15.07.2018 12:43:28	ActiveDirectory_DomainService	2089	Sicherung
Warnung	15.07.2018 12:43:28	ActiveDirectory_DomainService	2089	Sicherung
Warnung	15.07.2018 12:43:28	ActiveDirectory_DomainService	2089	Sicherung
Informationen	15.07.2018 11:58:29	ActiveDirectory_DomainService	1869	Globaler Katalog
Informationen	15.07.2018 11:58:29	NTDS ISAM	701	Onlinedefragmentier...
Informationen	15.07.2018 11:58:29	NTDS ISAM	700	Onlinedefragmentier...
Informationen	15.07.2018 11:58:29	NTDS ISAM	326	Allgemein
Informationen	15.07.2018 11:58:29	NTDS ISAM	105	Allgemein
Informationen	15.07.2018 11:58:29	NTDS ISAM	102	Allgemein
Informationen	15.07.2018 11:48:28	ActiveDirectory_DomainService	1104	Konsistenzprüfung
Warnung	15.07.2018 11:48:28	ActiveDirectory_DomainService	1308	Konsistenzprüfung
Informationen	15.07.2018 11:43:58	ActiveDirectory_DomainService	1394	Dienststeuerung
Informationen	15.07.2018 11:43:28	ActiveDirectory_DomainService	1000	Dienststeuerung
Warnung	15.07.2018 11:43:28	ActiveDirectory_DomainService	2886	LDAP-Schnittstelle

Ereignis 2089, ActiveDirectory_DomainService

Allgemein Details

Diese Verzeichnispartition wurde mindestens seit der folgenden Anzahl an Tagen nicht mehr gesichert.

Verzeichnispartition:
DC=DomainDnsZones,DC=nsedv,DC=de

"Sicherungsintervall (Tagen):
90

Protokollname: Directory Service
Quelle: ActiveDirectory_DomainServ Protokolliert: 15.07.2018 12:43:28
Ereignis-ID: 2089 Aufgabenkategorie: Sicherung
Ebene: Warnung Schlüsselwörter: Klassisch
Benutzer: ANONYMOUS-ANMELDUNG Computer: DC01.ndsedv.de
Vorgangscod: Info
Weitere Informationen: [Onlinehilfe](#)

