

# Systemdokumentation für DC

## Dokumentversionen

Ermittlungszeit: 03.01.2014 15:56:21

## Zusammenfassung

Betriebssystem: Microsoft Windows Server 2008 R2 Datacenter

Service Pack: Service Pack 1

NetBIOS-Name: DC

FQDN: dc.smm.local

Rollen: DC, File

Identifikationsnummer: VMware-56 4d 96 69 81 8e 96 51-0b 75 05 b2 21 03 ea 3a

## Inhaltsverzeichnis

<b>1.</b>	<b>System-Information</b>	<b>3</b>
<b>2.</b>	<b>Hardware-Plattform</b>	<b>3</b>
2.1.	Allgemeine Informationen	3
2.2.	BIOS-Informationen	4
<b>3.</b>	<b>Software-Plattform</b>	<b>4</b>
3.1.	Allgemeine Informationen	4
3.2.	Installierte Patches	4
3.3.	Derzeit installierte Programme (von Windows Installer)	9
3.4.	Derzeit installierte Programme (aus der Registry)	10
<b>4.</b>	<b>Storage</b>	<b>10</b>
4.1.	Allgemeine Informationen	10
<b>5.</b>	<b>Netzwerkconfiguration</b>	<b>11</b>
5.1.	IP-Konfiguration	11
5.2.	IP-Routen	11
<b>6.</b>	<b>Weitere Konfiguration</b>	<b>11</b>
6.1.	Eventlog-Dateien	11
6.2.	Drucker	13
6.3.	Regionale Einstellungen	13
6.4.	Laufende Prozesse	13
6.5.	Dienste	15
6.6.	Freigaben	24
6.7.	Systemstart-Kommandos	25
6.8.	Windows Registry	25



DC

## 1. System-Information

## 2. Hardware-Plattform

### 2.1. Allgemeine Informationen

Hersteller: VMware, Inc.

Produktname: VMware Virtual Platform

Identifikationsnummer: VMware-56 4d 96 69 81 8e 96 51-0b 75 05 b2 21 03 ea 3a

Gehäuse: Other

### Prozessor

Prozessor: Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz

Beschreibung: Intel64 Family 6 Model 45 Stepping 7

Takt (MHz): 2000

L2 Cache-Größe (Kb): 0

Externer Takt (MHz):

Anzahl der Prozessoren: 2

Hyper-Threading-System: Falsch

### Speicher

Gesamtspeicher (Mb): 16384

Bank	Kapazität	Bauform	Typ
RAM slot #0	16384	DIMM	DRAM

### CD-ROM

Name	Laufwerk	Hersteller
NECVMWar VMware IDE CDR10 ATA Device	D:	(Standard-CD-ROM-Laufwerke)

### Video-Controller

Name	Adapter-RAM	Kompatibilität
VMware SVGA 3D	8	VMware, Inc.

DC

## 2.2. BIOS-Informationen

BIOS-Version: INTEL - 6040000

SMBIOS Version: 6.00 (2,4)

BIOS-Charakteristiken: ISA is supported, PCI is supported, PC Card (PCMCIA) is supported, Plug and Play is supported, APM is supported, BIOS is Upgradable (Flash), BIOS shadowing is allowed, ESCD support is available, Boot from CD is supported, Selectable Boot is supported, EDD (Enhanced Disk Drive) Specification is supported, Int 5h, Print Screen Service is supported, Int 9h, 8042 Keyboard services are supported, Int 14h, Serial Services are supported, Int 17h, printer services are supported, Int 10h, CGA/Mono Video Services are supported, ACPI supported, Smart Battery supported, Unknown (Undocumented), Unknown (Undocumented), Unknown (Undocumented), Unknown (Undocumented), Unknown (Undocumented), Unknown (Undocumented)

## 3. Software-Plattform

### 3.1. Allgemeine Informationen

OS-Name: Microsoft Windows Server 2008 R2 Datacenter

Computer-Rolle: Domain Controller (PDC Emulator)

Domänentyp: domain

Domänen-Name: smm.local

Installationsort: C:\Windows

OS-Sprache: German

Installationsdatum: 19.06.2013 14:00:33

Letzter angemeldeter Nutzer: SMM\

### 3.2. Installierte Patches

Patch ID	Beschreibung	Installationsdatum
KB981391	Update	6/20/2013
KB981392	Update	6/20/2013
KB977236	Update	6/20/2013
KB981111	Update	6/20/2013
KB977238	Update	6/20/2013
KB2849697	Update	11/20/2013
KB2849697	Update	11/20/2013
KB2849696	Update	11/20/2013
KB2849696	Update	11/20/2013
KB2841134	Update	11/20/2013
KB2841134	Update	11/20/2013

DC

KB977239	Update	6/20/2013
KB2670838	Update	6/20/2013
KB2592687	Update	6/20/2013
KB981390	Update	6/20/2013
KB2386667	Update	6/20/2013
KB2425227	Security Update	6/20/2013
KB2506014	Update	6/20/2013
KB2506212	Security Update	6/20/2013
KB2506928	Update	6/20/2013
KB2509553	Security Update	6/20/2013
KB2511455	Security Update	6/20/2013
KB2515325	Update	6/20/2013
KB2529073	Update	6/20/2013
KB2533552	Update	6/20/2013
KB2536275	Security Update	6/20/2013
KB2536276	Security Update	6/20/2013
KB2541014	Update	6/20/2013
KB2544893	Security Update	6/20/2013
KB2545698	Update	6/20/2013
KB2547666	Update	6/20/2013
KB2552343	Update	6/20/2013
KB2560656	Security Update	6/20/2013
KB2563227	Update	6/20/2013
KB2564958	Security Update	6/20/2013
KB2570947	Security Update	6/20/2013
KB2574819	Update	6/20/2013
KB2584146	Security Update	6/20/2013
KB2585542	Security Update	6/20/2013
KB2603229	Update	6/20/2013
KB2604115	Security Update	6/20/2013
KB2607047	Update	6/20/2013
KB2608658	Update	6/20/2013
KB2618451	Security Update	6/20/2013
KB2620704	Security Update	6/20/2013

DC

KB2621440	Security Update	6/20/2013
KB2631813	Security Update	6/20/2013
KB2636573	Update	6/20/2013
KB2640148	Update	6/20/2013
KB2643719	Security Update	6/20/2013
KB2644615	Security Update	6/20/2013
KB2645640	Security Update	6/20/2013
KB2647170	Security Update	8/7/2013
KB2647753	Update	6/20/2013
KB2653956	Security Update	6/20/2013
KB2654428	Security Update	6/20/2013
KB2655992	Security Update	6/20/2013
KB2656356	Security Update	6/20/2013
KB2658846	Security Update	6/20/2013
KB2659262	Security Update	6/20/2013
KB2660075	Update	6/20/2013
KB2667402	Security Update	6/20/2013
KB2676562	Security Update	6/20/2013
KB2685811	Update	6/20/2013
KB2685813	Update	6/20/2013
KB2685939	Security Update	6/20/2013
KB2690533	Security Update	6/20/2013
KB2691442	Security Update	6/20/2013
KB2698365	Security Update	6/20/2013
KB2699779	Update	6/20/2013
KB2705219	Security Update	6/20/2013
KB2706045	Security Update	6/20/2013
KB2709630	Update	6/20/2013
KB2709981	Update	6/20/2013
KB2712808	Security Update	6/20/2013
KB2718704	Update	6/20/2013
KB2719857	Update	6/20/2013
KB2726535	Update	6/20/2013
KB2729094	Update	6/20/2013

DC

KB2729452	Security Update	6/20/2013
KB2732059	Update	6/20/2013
KB2736422	Security Update	7/11/2013
KB2742599	Security Update	6/20/2013
KB2743555	Security Update	6/20/2013
KB2749655	Update	6/20/2013
KB2750841	Update	6/20/2013
KB2753842	Security Update	6/20/2013
KB2756921	Security Update	7/11/2013
KB2757638	Security Update	6/20/2013
KB2758857	Security Update	6/20/2013
KB2761217	Update	6/20/2013
KB2763523	Update	6/20/2013
KB2765809	Security Update	6/20/2013
KB2770660	Security Update	6/20/2013
KB2772930	Security Update	7/11/2013
KB2779562	Update	6/20/2013
KB2785220	Security Update	6/20/2013
KB2786081	Update	6/20/2013
KB2786400	Update	6/20/2013
KB2789645	Security Update	6/20/2013
KB2790113	Security Update	6/20/2013
KB2791765	Update	6/20/2013
KB2798162	Update	6/20/2013
KB2804579	Security Update	6/20/2013
KB2806748	Update	7/11/2013
KB2807986	Security Update	6/20/2013
KB2808679	Update	6/20/2013
KB2813170	Security Update	6/20/2013
KB2813347	Security Update	6/20/2013
KB2813430	Security Update	6/20/2013
KB2820197	Security Update	6/20/2013
KB2820331	Update	6/20/2013
KB2829361	Security Update	6/20/2013

DC

KB2830290	Security Update	6/20/2013
KB2832414	Security Update	7/11/2013
KB2833946	Security Update	7/11/2013
KB2834140	Update	6/20/2013
KB2834886	Security Update	7/11/2013
KB2835361	Security Update	7/11/2013
KB2836502	Update	6/20/2013
KB2836942	Update	7/25/2013
KB2836943	Update	9/12/2013
KB2838727	Security Update	6/20/2013
KB2839894	Security Update	6/20/2013
KB2840149	Security Update	6/20/2013
KB2840631	Security Update	7/11/2013
KB2844286	Security Update	8/15/2013
KB2845690	Security Update	6/20/2013
KB2847311	Security Update	11/14/2013
KB2849470	Security Update	8/15/2013
KB2850851	Security Update	7/11/2013
KB2853587	Security Update	9/12/2013
KB2853952	Update	9/12/2013
KB2859537	Security Update	8/15/2013
KB2861191	Security Update	11/14/2013
KB2861698	Security Update	11/14/2013
KB2861855	Security Update	8/15/2013
KB2862152	Security Update	11/14/2013
KB2862330	Security Update	11/14/2013
KB2862335	Security Update	11/14/2013
KB2862966	Security Update	8/15/2013
KB2863058	Update	8/15/2013
KB2863240	Security Update	11/14/2013
KB2864058	Security Update	11/14/2013
KB2864202	Security Update	11/14/2013
KB2868038	Security Update	11/14/2013
KB2868116	Update	9/12/2013



DC

KB2868623	Security Update	8/15/2013
KB2868626	Security Update	11/14/2013
KB2868725	Security Update	11/14/2013
KB2872339	Security Update	9/12/2013
KB2875783	Security Update	11/14/2013
KB2876284	Security Update	11/14/2013
KB2876315	Security Update	9/12/2013
KB2876331	Security Update	11/14/2013
KB2882822	Update	11/14/2013
KB2883150	Security Update	11/14/2013
KB2884256	Security Update	11/14/2013
KB2887069	Security Update	12/12/2013
KB2888049	Update	11/14/2013
KB2891804	Update	12/12/2013
KB2892074	Security Update	12/12/2013
KB2893294	Security Update	12/12/2013
KB2893519	Update	11/14/2013
KB2893984	Security Update	12/12/2013
KB2898785	Security Update	12/12/2013
KB2900986	Security Update	11/14/2013
KB2904266	Update	12/12/2013
KB2913152	Update	12/12/2013
KB976902	Update	11/21/2010
KB982018	Update	6/20/2013

### 3.3. Derzeit installierte Programme (von Windows Installer)

Name	Hersteller	Version	Installationsdatum
GFI LanGuard 11 Agent	GFI Software Ltd	11.0.2012.0717	20130813
Java 7 Update 45	Oracle	7.0.450	20131017
Java Auto Updater	Sun Microsystems, Inc.	2.1.9.8	20131002
Managed Antivirus	GFI Software	6.2.5528	20130924
Microsoft .NET Framework 4.5.1	Microsoft Corporation	4.5.50938	20131128

DC

Microsoft .NET Framework 4.5.1 (DEU)	Microsoft Corporation	4.5.50938	20131129
Microsoft Silverlight	Microsoft Corporation	5.1.20913.0	20131009
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	Microsoft Corporation	9.0.30729.6161	20130619
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	Microsoft Corporation	9.0.30729.4148	20130619
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	Microsoft Corporation	9.0.30729.6161	20130814
MSXML 4.0 SP2 (KB954430)	Microsoft Corporation	4.20.9870.0	20130925
MSXML 4.0 SP2 (KB973688)	Microsoft Corporation	4.20.9876.0	20130925
VMware Tools	VMware, Inc.	9.0.5.21789	20130619

### 3.4. Derzeit installierte Programme (aus der Registry)

Name	Version
Microsoft .NET Framework 4.5.1	4.5.50938
Microsoft .NET Framework 4.5.1 (Deutsch)	4.5.50938

## 4. Storage

### 4.1. Allgemeine Informationen

#### VMware Virtual disk SCSI Disk Device - \\.\PHYSICALDRIVE0

Interface: SCSI

Gesamtdatenträgergröße (Gb): 100

C: 99,9 Gb (54,87 Gb Frei) NTFS

E: 400 Gb (220,57 Gb Frei) NTFS

DC

## 5. Netzwerkkonfiguration

### 5.1. IP-Konfiguration

#### Netzwerkadapter 1

Beschreibung: vmxnet3 Ethernet Adapter

MAC: 00:0C:29:03:EA:3A

IP-Adresse: 192.168.5.200/255.255.255.0, fe80::22:2d6:10bf:fa57/64

Gateway: 192.168.5.254

DNS-Server: 192.168.5.11

### 5.2. IP-Routen

Ziel	Subnetzmaske	Gateway
0.0.0.0	0.0.0.0	192.168.5.254
127.0.0.0	255.0.0.0	0.0.0.0
127.0.0.1	255.255.255.255	0.0.0.0
127.255.255.255	255.255.255.255	0.0.0.0
192.168.5.0	255.255.255.0	0.0.0.0
192.168.5.200	255.255.255.255	0.0.0.0
192.168.5.255	255.255.255.255	0.0.0.0
224.0.0.0	240.0.0.0	0.0.0.0
224.0.0.0	240.0.0.0	0.0.0.0
255.255.255.255	255.255.255.255	0.0.0.0
255.255.255.255	255.255.255.255	0.0.0.0

## 6. Weitere Konfiguration

### 6.1. Eventlog-Dateien

#### Active Directory Web Services

Datei: C:\Windows\System32\Winevt\Logs\Active Directory Web Services.evtx

Maximalgröße (Mb): 1,00390625

Richtlinie zum Überschreiben: Bei Bedarf

#### Application

Datei: C:\Windows\System32\Winevt\Logs\Application.evtx

Maximalgröße (Mb): 20

Richtlinie zum Überschreiben: Bei Bedarf

#### DFS Replication

Datei: C:\Windows\System32\Winevt\Logs\DFS Replication.evtx

DC

Maximalgröße (Mb): 14,8125

Richtlinie zum Überschreiben: Bei Bedarf

### **Directory Service**

Datei: C:\Windows\System32\Winevt\Logs\Directory Service.evtx

Maximalgröße (Mb): 1,00390625

Richtlinie zum Überschreiben: Bei Bedarf

### **DNS Server**

Datei: C:\Windows\System32\Winevt\Logs\DNS Server.evtx

Maximalgröße (Mb): 16

Richtlinie zum Überschreiben: Bei Bedarf

### **File Replication Service**

Datei: C:\Windows\System32\Winevt\Logs\File Replication Service.evtx

Maximalgröße (Mb): 1,00390625

Richtlinie zum Überschreiben: Bei Bedarf

### **HardwareEvents**

Datei: C:\Windows\System32\Winevt\Logs\HardwareEvents.evtx

Maximalgröße (Mb): 20

Richtlinie zum Überschreiben: Bei Bedarf

### **Internet Explorer**

Datei: C:\Windows\System32\Winevt\Logs\Internet Explorer.evtx

Maximalgröße (Mb): 1,00390625

Richtlinie zum Überschreiben: Bei Bedarf

### **Key Management Service**

Datei: C:\Windows\System32\Winevt\Logs\Key Management Service.evtx

Maximalgröße (Mb): 20

Richtlinie zum Überschreiben: Bei Bedarf

### **MSExchange Management**

Datei: C:\Windows\System32\Winevt\Logs\MSExchange Management.evtx

Maximalgröße (Mb): 1,00390625

Richtlinie zum Überschreiben: Bei Bedarf

### **Security**

Datei: C:\Windows\System32\Winevt\Logs\Security.evtx

Maximalgröße (Mb): 128

Richtlinie zum Überschreiben: Bei Bedarf

DC

## System

Datei: C:\Windows\System32\Winevt\Logs\System.evtx

Maximalgröße (Mb): 20

Richtlinie zum Überschreiben: Bei Bedarf

## Windows PowerShell

Datei: C:\Windows\System32\Winevt\Logs\Windows PowerShell.evtx

Maximalgröße (Mb): 15

Richtlinie zum Überschreiben: Bei Bedarf

## 6.2. Drucker

Druckwarteschlangenverzeichnis: C:\Windows\system32\spool\PRINTERS

Name	Treiber	Anschluss
Microsoft XPS Document Writer	Microsoft XPS Document Writer	XPSPort:

## 6.3. Regionale Einstellungen

Zeitzone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

## 6.4. Laufende Prozesse

Name	Ausführbare Datei
csrss.exe	C:\Windows\system32\csrss.exe
csrss.exe	C:\Windows\system32\csrss.exe
dfsrs.exe	C:\Windows\system32\DFSRs.exe
dfssvc.exe	C:\Windows\system32\dfssvc.exe
dllhost.exe	C:\Windows\system32\dllhost.exe
dns.exe	C:\Windows\system32\dns.exe
dwm.exe	C:\Windows\system32\Dwm.exe
explorer.exe	C:\Windows\Explorer.EXE
ismserv.exe	C:\Windows\System32\ismserv.exe
Inssatt.exe	C:\PROGRA~2\ADVANC~1\patchman\Inssatt.exe
LogonUI.exe	C:\Windows\system32\LogonUI.exe
lsass.exe	C:\Windows\system32\lsass.exe
lsm.exe	C:\Windows\system32\lsm.exe
Microsoft.ActiveDirectory.WebServices.exe	C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe

DC

msdtc.exe	C:\Windows\System32\msdtc.exe
ntfrs.exe	C:\Windows\system32\ntfrs.exe
SBAMSvc.exe	C:\PROGRA~2\ADVANC~1\managedav\ SBAMSvc.exe
SBAMTray.exe	C:\Program Files (x86)\Advanced Monitoring Agent\managedav\SBAMTray.exe
services.exe	C:\Windows\system32\services.exe
smss.exe	
spoolsv.exe	C:\Windows\System32\spoolsv.exe
svchost.exe	C:\Windows\system32\svchost.exe
svchost.exe	C:\Windows\system32\svchost.exe
svchost.exe	C:\Windows\System32\svchost.exe
svchost.exe	C:\Windows\system32\svchost.exe
svchost.exe	C:\Windows\system32\svchost.exe
svchost.exe	C:\Windows\System32\svchost.exe
svchost.exe	C:\Windows\system32\svchost.exe
svchost.exe	C:\Windows\system32\svchost.exe
svchost.exe	C:\Windows\System32\svchost.exe
svchost.exe	C:\Windows\system32\svchost.exe
svchost.exe	C:\Windows\system32\svchost.exe
svchost.exe	C:\Windows\System32\svchost.exe
svchost.exe	C:\Windows\system32\svchost.exe
System	
System Idle Process	
taskhost.exe	C:\Windows\system32\taskhost.exe
TeamViewer.exe	c:\program files (x86)\teamviewer\version8\TeamViewer. exe
TeamViewer.exe	C:\Program Files (x86)\TeamViewer\Version9\TeamViewer .exe
TeamViewer_Service.exe	C:\Program Files (x86)\TeamViewer\Version8\TeamViewer _Service.exe
TeamViewer_Service.exe	C:\Program Files (x86)\TeamViewer\Version9\TeamViewer _Service.exe

DC

tv_w32.exe	C:\Program Files (x86)\TeamViewer\Version8\tv_w32.exe
tv_x64.exe	C:\Program Files (x86)\TeamViewer\Version8\tv_x64.exe
vds.exe	C:\Windows\System32\vds.exe
vmtoolsd.exe	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
vmtoolsd.exe	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
winagent.exe	C:\Program Files (x86)\Advanced Monitoring Agent\winagent.exe
wininit.exe	C:\Windows\system32\wininit.exe
winlogon.exe	C:\Windows\system32\winlogon.exe
WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.e xe
WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.e xe

## 6.5. Dienste

Name	Startmodus	Gestartet	Anmelden als
Active Directory- Domänendienste	Auto	True	LocalSystem
Active Directory- Webdienste	Auto	True	LocalSystem
Advanced Monitoring Agent	Auto	True	LocalSystem
Anmeldedienst	Auto	True	LocalSystem
Anmeldeinformatio nsverwaltung	Manual	False	LocalSystem
Anschlussumleitun g für Remotedesktopdie nst im Benutzermodus	Manual	True	localSystem
Anwendungserfahr ung	Manual	False	localSystem
Anwendungsidentit ät	Manual	False	NT Authority\LocalServ ice

## DC

Anwendungsinformationen	Manual	False	LocalSystem
Anwendungsverwaltung	Manual	False	LocalSystem
Arbeitsstationsdienst	Auto	True	NT AUTHORITY\NetworkService
ASP.NET-Zustandsdienst	Manual	False	NT AUTHORITY\NetworkService
Aufgabenplanung	Auto	True	LocalSystem
Automatische Konfiguration (verkabelt)	Manual	False	localSystem
Basisfiltermodul	Auto	True	NT AUTHORITY\LocalService
Benachrichtigungsdienst für Systemereignisse	Auto	True	LocalSystem
Benutzerprofildienst	Auto	True	LocalSystem
Blockebenen-Sicherungsmodul	Manual	False	LocalSystem
CNG-Schlüsselisolation	Manual	False	LocalSystem
COM+-Ereignissystem	Auto	True	NT AUTHORITY\LocalService
COM+-Systemanwendung	Manual	True	LocalSystem
Computerbrowser	Disabled	False	LocalSystem
Dateireplikationsdienst	Auto	True	LocalSystem
DCOM-Server-Prozessstart	Auto	True	LocalSystem
Defragmentierung	Manual	False	localSystem
DFS-Namespace	Auto	True	LocalSystem
DFS-Replikation	Auto	True	LocalSystem



## DC

DHCP-Client	Auto	True	NT Authority\LocalService
DHCP-Server	Auto	True	NT AUTHORITY\NetworkService
Diagnosediensthost	Manual	False	NT AUTHORITY\LocalService
Diagnoserichtlinien dienst	Auto	True	NT AUTHORITY\LocalService
Diagnosesystemho st	Manual	False	LocalSystem
Distributed Transaction Coordinator	Auto	True	NT AUTHORITY\NetworkService
DNS-Client	Auto	True	NT AUTHORITY\NetworkService
DNS-Server	Auto	True	LocalSystem
Druckwarteschlang e	Auto	True	LocalSystem
Enumeratordienst für tragbare Geräte	Manual	False	LocalSystem
Erkennung interaktiver Dienste	Manual	False	LocalSystem
Extensible Authentication- Protokoll	Manual	False	localSystem
Funktionssuchanbi eter-Host	Manual	False	NT AUTHORITY\LocalService
Funktionssuche- Ressourcenveröff entlichung	Manual	False	NT AUTHORITY\LocalService
Gatewaydienst auf Anwendungsebene	Manual	False	NT AUTHORITY\LocalService

## DC

Gemeinsame Nutzung der Internetverbindung	Disabled	False	LocalSystem
Geschützter Speicher	Manual	False	LocalSystem
GFI LanGuard 11 Attendant Service	Auto	True	LocalSystem
Gruppenrichtlinienclient	Auto	True	LocalSystem
Hilfsprogramm für spezielle Verwaltungskonsolen	Manual	False	LocalSystem
IKE- und AuthIP IPsec-Schlüsselerstellungsmodule	Auto	True	LocalSystem
Integritätsschlüssel- und Zertifikatverwaltung	Manual	False	localSystem
Intelligenter Hintergrundübertragungsdienst	Manual	True	LocalSystem
Internet Explorer ETW Collector Service	Manual	False	LocalSystem
IP-Hilfsdienst	Auto	True	LocalSystem
IPsec-Richtlinien-Agent	Manual	True	NT Authority\NetworkService
Kerberos-Schlüsselverteilungsscenter	Auto	True	LocalSystem
Konfiguration für Remotedesktops	Manual	True	localSystem
Kryptografiedienste	Auto	True	NT Authority\NetworkService
KtmRm für Distributed	Manual	False	NT AUTHORITY\NetworkService

DC

Transaction  
Coordinator

Leistungsindikator- DLL-Host	Manual	False	NT AUTHORITY\Local Service
Leistungsprotokolle und -warnungen	Manual	False	NT AUTHORITY\Local Service
Managed Antivirus	Auto	True	LocalSystem
Microsoft .NET Framework NGEN v2.0.50727_X64	Manual	False	LocalSystem
Microsoft .NET Framework NGEN v2.0.50727_X86	Manual	False	LocalSystem
Microsoft .NET Framework NGEN v4.0.30319_X64	Auto	False	LocalSystem
Microsoft .NET Framework NGEN v4.0.30319_X86	Auto	False	LocalSystem
Microsoft iSCSI- Initiator-Dienst	Manual	False	LocalSystem
Microsoft- Softwareschattenko pie-Anbieter	Manual	False	LocalSystem
Mozilla Maintenance Service	Manual	False	LocalSystem
Multimediaklassenp laner	Manual	False	LocalSystem
NAP-Agent (Network Access Protection)	Manual	False	NT AUTHORITY\Netw orkService
Net.Msmq- Listeneradapter	Disabled	False	NT AUTHORITY\Netw orkService
Net.Pipe- Listeneradapter	Disabled	False	NT AUTHORITY\Local Service

DC

Net.Tcp- Listeneradapter	Disabled	False	NT AUTHORITY\Local Service
Net.Tcp- Portfreigabedienst	Disabled	False	NT AUTHORITY\Local Service
Netzwerklistendien- st	Manual	True	NT AUTHORITY\Local Service
Netzwerkspeicher- Schnittstellendienst	Auto	True	NT Authority\LocalServ ice
Netzwerkverbindun- gen	Manual	True	LocalSystem
NLA (Network Location Awareness)	Auto	True	NT AUTHORITY\Netw orkService
Plug & Play	Auto	True	LocalSystem
PnP-X-IP- Busenumeration	Disabled	False	LocalSystem
RAS- Verbindungsverwalt- ung	Manual	False	localSystem
Registrierungsdienst für Microsoft Fibre Channel- Plattform	Manual	False	NT AUTHORITY\Local Service
Remotedesktopdien- ste	Manual	True	NT Authority\NetworkS ervice
Remoteprozedurauf- ruf (RPC)	Auto	True	NT AUTHORITY\Netw orkService
Remoteregistrierun- g	Auto	True	NT AUTHORITY\Local Service
Richtlinie zum Entfernen der Smartcard	Manual	False	LocalSystem
Richtlinienergebnis- satanbieter	Manual	False	LocalSystem
Routing und RAS	Disabled	False	localSystem

## DC

RPC-Endpunktzuordnung	Auto	True	NT AUTHORITY\NetworkService
RPC-Locator	Manual	False	NT AUTHORITY\NetworkService
Sekundäre Anmeldung	Manual	False	LocalSystem
Server	Auto	True	LocalSystem
Server für Threadsortierung	Manual	False	NT AUTHORITY\LocalService
Shellhardwareerkennung	Auto	True	LocalSystem
Sicherheitskonto-Manager	Auto	True	LocalSystem
Sitzungs-Manager für Desktopfenster-Manager	Auto	True	localSystem
Smartcard	Manual	False	NT AUTHORITY\LocalService
SNMP-Trap	Manual	False	NT AUTHORITY\LocalService
Software Protection	Auto	False	NT AUTHORITY\NetworkService
SPP-Benachrichtigungsdienst	Manual	False	NT AUTHORITY\LocalService
SSDP-Suche	Disabled	False	NT AUTHORITY\LocalService
SSTP-Dienst	Manual	False	NT Authority\LocalService
Standortübergreifen der Messagingdienst	Auto	True	LocalSystem
Stromversorgung	Auto	True	LocalSystem

DC

TCP/IP-NetBIOS-Hilfsdienst	Auto	True	NT AUTHORITY\Local Service
TeamViewer 8	Auto	True	LocalSystem
TeamViewer 9	Auto	True	LocalSystem
Telefonie	Manual	False	NT AUTHORITY\NetworkService
TPM-Basisdienste	Manual	False	NT AUTHORITY\Local Service
Überwachung verteilter Verknüpfungen (Client)	Manual	False	LocalSystem
Unterstützung in der Systemsteuerung unter Lösungen für Probleme	Manual	False	localSystem
UPnP-Gerätehost	Disabled	False	NT AUTHORITY\Local Service
Verbindungsschicht - Topologieerkennungsgs-Zuordnungsprogramm	Manual	False	NT AUTHORITY\Local Service
Verschlüsselndes Dateisystem (EFS)	Manual	False	LocalSystem
Verwaltung für automatische RAS-Verbindung	Manual	False	localSystem
Virtueller Datenträger	Manual	True	LocalSystem
VMTools	Auto	True	LocalSystem
VMware Snapshot Provider	Manual	False	LocalSystem
Volumeschattenkopie	Manual	False	LocalSystem

DC

Windows CardSpace	Manual	False	LocalSystem
Windows Driver Foundation - Benutzermodus-Treiberframework	Manual	False	LocalSystem
Windows Installer	Manual	True	LocalSystem
Windows Modules Installer	Manual	False	localSystem
Windows Presentation Foundation-Schriftartcache 3.0.0.0	Manual	False	NT Authority\LocalService
Windows Update	Auto	True	LocalSystem
Windows-Audio	Manual	False	NT AUTHORITY\Local Service
Windows-Audio-Endpunkterstellung	Manual	False	LocalSystem
Windows-Dienst für Schriftartencache	Auto	True	NT AUTHORITY\Local Service
Windows-Ereignisprotokoll	Auto	True	NT AUTHORITY\Local Service
Windows-Ereignissammlung	Manual	False	NT AUTHORITY\NetworkService
Windows-Farbsystem	Manual	False	NT AUTHORITY\Local Service
Windows-Fehlerberichterstattungsdienst	Manual	False	localSystem
Windows-Firewall	Auto	True	NT Authority\LocalService
Windows-Remoteverwaltung (WS-Verwaltung)	Auto	True	NT AUTHORITY\NetworkService

DC

Windows-Verwaltungsinstrumentation	Auto	True	localSystem
Windows-Zeitgeber	Manual	True	NT AUTHORITY\Local Service
WinHTTP-Web Proxy Auto-Discovery-Dienst	Manual	True	NT AUTHORITY\Local Service
WMI-Leistungsadapter	Manual	False	localSystem
Zertifikatverteilung	Manual	True	LocalSystem
Zugriff auf Eingabegeräte	Manual	False	LocalSystem

## 6.6. Freigaben

Name	Pfad	Beschreibung
ADMIN\$	C:\Windows	Remoteverwaltung
Alle-NEU	E:\Alle-NEU	
C\$	C:\	Standardfreigabe
Daten	E:\Daten	
daten\$	E:\Daten	
E\$	E:\	Standardfreigabe
hpfindel	E:\User\hpfindel	
IPC\$		Remote-IPC
klicktel	E:\klicktel	
NETLOGON	C:\Windows\SYSTEM32\sysvol\smm.local\SCRIPTS	Ressource für Anmeldeserver
print\$	C:\WINDOWS\system32\spool\drivers	Druckertreiber
prnproc\$	C:\WINDOWS\system32\spool\PRTPROCS	
Public	C:\Users\Public	
Scanner	C:\Scanner	
Support	E:\Support	
Swyxbackup\$	E:\Swyxbackup	



DC

SYSVOL	C:\Windows\SYSVOL\sysvol	Ressource für Anmeldeserver
User\$	E:\User	
Users	C:\Users	

## 6.7. Systemstart-Kommandos

<b>Nutzer</b>	<b>Name</b>	<b>Kommando</b>
Public	VMware User Process	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

## 6.8. Windows Registry

Aktuelle Registry-Größe (Mb): 68

Maximale Registry-Größe (Mb): 2048