W2K8 and Newer Technical Reference

Documentname: OS W2K8 and Newer - Tech_Ref.docx
Last update: 07.06.2020
Author: A. Balogh

Inhalt

Einführung ... 8
TOOLS ... 8
PowerShell ... 9
VBScript ... 10
Windows 2008 Core Installation ... 11
Installieren von Server Core ... 11
Installieren eines Domänencontrollers ... 12
Gesamtstruktur ... 12
Active Directory-Migrationstoll (ADMT) ... 14
Installieren einer neuen W2k8-Gesamtstruktur ... 14
Installieren weiterer Domänencontroller in einer Domäne ... 14
Installieren einer neuen untergeordneten W2k8-Server-Domäne ... 15
Installieren einer neuen Domänenstruktur ... 15
Installation eines RODC für Zweigstellen ... 15
Installieren der AD DS von einem Medium ... 15
Entfernen eines Domänencontrollers ... 16
Konfigurieren von Betriebsmastern ... 17
Domänennamenmaster ... 18
Schemamaster ... 18
RID-Master ... 19
Infrastrukturmaster ... 19
Phantomobjekt ... 19

PDC-Emulator ... **19**
Platzieren von Betriebsmastern ... **20**
Übertragen von Betriebsmaster-Rollen ... **20**
Funktionsebenen ... **20**
Domänenfunktionsebenen ... 20
Gesamtstrukturfunktionsebenen ... 21
Konfigurieren der DFS-Replikation von SYSVOL ... ***22***
Standorte und Replikation ... ***23***
Konfigurieren von Standorten und Subnetzen ... **23**
Replikationsdatenverkehr ... 23
Dienstlokalisierung (SRV-Einträge) ... 23
Standorte erstellen ... 23
Subnetzobjekt ... 23
Globaler Katalog und Anwendungsverzeichnispartition ... ***24***
Globaler Katalog (Global Catalog, GC) ... **24**
Universelle Gruppenmitgliedschaft (UGMC) ... **24**
Anwendungsverzeichnispartitionen ... **25**
Konfigurieren der Replikation ... ***25***
Verbindungsobjekte ... **25**
Konsistenzprüfung (KCC) ... **25**
Benachrichtigung ... **26**
Abfragen (Polling) ... **26**
Standortverknüpfungen ... **26**
Standortverknüpfungsbrücken ... 26
Standortverknüpfungskosten ... 26
Replikationsprotokolle ... **26**
Replikationshäufigkeit ... **27**
Replikationzeitpläne ... **27**
Überwachen der Replikation ... **27**
Repadmin.exe ... 27
Dcdiag.exe ... 27
Bridgeheadserver ... **27**
Business Continuity ... ***28***
Acctinfo.dll ... **28**
ALTools.exe ... **28**
Specops Gpupdate ... **28**
Verzeichnisschutzmassnahmen ... **28**
Quest Object Restore for Active Directory ... **29**
Windows Server-Sicherung ... **29**
wbadmin.exe (Windows Server Sicherung) ... 30
Wiederherstellung mit WinRE ... 30
Autorisierende und nicht autorisierende Wiederherstellung ... 30

Verwaltung der Systemleistung *30*
Task-Manager **30**
Swapping/Paging 30
Ereignisanzeige **30**
Windows-Zuverlässigkeitsüberwachung **31**
Windows-Leistungsüberwachung **31**
Windows-Systemressourcen-Manager (WSRM) **31**
Active Directory Lightweight Directory Services (AD LDS) *32*
Active Directory-Zertifikatdienste (AD CS) und PKI *33*
Unternehmenszertifizierungsstellen (CA) **34**
Active Directory-Rechteverwaltungsdienst (AD RMS) *34*
Die Phasen der Implementierung **35**
Bereitstellungsszenarien **35**
Die Verwaltungsrollen der AD RMS: **35**
Dienstverbindungspunkt **36**
Datenbank **36**
Active Directory-Verbunddienste (AD FS) *36*
Upgrades **37**
Terminaldienste *38*
Remotedesktop **38**
Configuration: Remotedesktopverbindung 38
Benutzerkonten *38*
Gruppen *39*
Verteilergruppen **39**
Sicherheitsgruppen **39**
Gruppenbereich **39**
Lokal 39
Domänenlokale Gruppen 40
Global 40
Universal 40
Computer *40*
Voraussetzungen Computer zu Domäne hinzufügen **40**
Gruppenrichtlinien *40*
Richtlinieneinstellungen **41**
Gruppenrichtlinienobjekte **41**
ADMX Files **42**
Vererbung und Rangfolge **42**
Vererbung deaktivieren 42
Verknüpfung erzwingen 42
Sicherheitsfilter **42**

WMI-Filter **42**
Loopbackrichtlinienverarbeitung **43**
Richtlinienergebnissatz (RSoP) **43**
Gruppenrichtlinienergebnis-Assistent 43
Gruppenrichtlinienaktualisierung **43**
GPO-Replikation **44**
GPOs für den Helpdesk **44**
Softwareinstallation (GPSI) ***44***
zugewiesen 45
veröffentlichen 45
Sicherheitseinstellungen ***45***
Sicherheitsvorlage **45**
Secedit.exe 46
Scwcmd.exe 46
Überwachung **46**
Authentifizierung ***46***
Vertrauensstellung ***47***
Read-Only Domain Controller (RODC) ***47***
Voraussetzungen **48**
Windows-Bereitstellungsinfrastruktur ***49***
Windows Automated Installation Kit (AIK) **49**
Sysprep **50**
Produkt-DVD **50**
Netzwerkfreigabe AIK und WIM-Dateien **50**
Windows-Bereitstellungsdienste (WDS) **50**
Windows PE-CD erstellen **51**
System Center Configuration Manager (SCCM) ***52***
Windows-Aktivierungsinfrastruktur ***52***
Hypervisor ***54***
Hyper-V ***55***
Hardwarevoraussetzungen **56**
Virtual Server 2005 R2 SP1 ..... ***57***
Virtual PC 2007 ..... ***57***
Serverspeicher ***57***
Direct-Attached Storage (DAS) **57**
Network-Attached Storage (NAS) **58**
Storage-Area Networks (SAN) **58**
Fibre-Channel-SANs (FC) 59
iSCSI-SANs 59
Cluster ***59***

Round-Robin **59**
Netzwerklastenausgleich (NLB) **60**
Failover-Cluster **60**
Netzwerkübersicht ***61***
Rollen ***62***
Windows Remote Management ***62***
Netzwerk-Bridge ***62***
Windows CardSpace ***62***
New TCP/IP-Stack ***63***
IP ***64***
Adressbereiche **64**
Private Adressbereiche 64
Berechnung der Hostkapazität 64
Berechnung der Subnetze 64
Subnetmasken variabler Länge (VLSM-Technik) 65
Broadcastbereich 65
NETSH-Befehl 65
DHCP-Infrastruktur **65**
IPv6 ..... ***66***
Unicast, Multicast und Anycast **66**
Globale Adressen **66**
Verbindungslokale Adressen **66**
Eindeutige lokale Adressen **66**
Standortlokale Adressen **66**
ISATAP **67**
6to4 ..... **67**
Teredo **67**
Configuring IPv6 With the Netsh.exe Tool **67**
Configuring Addresses 67
Adding Default Gateways 67
Adding DNS Servers 68
Disabling IPv6 ..... **68**
Namensauflösung ***70***
Dynamische DNS-Server (DDNS) 70
DSN-Server mit Schreibzugriff 70
Schreibgeschützte DNS-Server 70
Split-Brain Syndrom 70
Whole-Brain 70
Round-Robin 70
Web Proxy Automatic Discovery Protocol (WPAD) 70
Footprinting 70
NetBIOS oder NetBIOS-über TCP/IP **70**
WINS 71
LMHOSTS 71

GlobalNames-Zone (GNZ) ... 71
Link Local Multicast Name Resolution (LLMNR) ... **71**
Peer Name Resolution (PNRP) ... **71**
Routing ... ***72***
IPSec ... ***72***
Sicherheitszuordnungen ... **72**
Network Adress Translation (NAT) ... ***72***
Internet Connection Sharing (ICS) ... **73**
Routing und RAS-Dienste (RRAS) ... **73**
Drahtlosnetzwerke ... ***73***
Remotenetzwerke ... ***74***
DFÜ-Verbindungen ... **74**
VPN-Verbindungen ... **74**
Secure Socket Tunneling Protocol (SSTP) ... 74
Windows Firewall & Netzwerkzugriffsschutz (NAP) ... ***74***
Network Access Protection (NAP) ... **74**
Policies ... 75
Windows Security Health Validator ... 76
Bootstrap Wireless Profile ... 76
Windows Server Update Services (WSUS) ... ***76***
Windows Update Dienst ... **76**
Ereignissweiterleitung ... ***77***
Sammelcomputer ... **77**
Weiterleitungscomputer ... **77**
Aktivieren der Remoteverwaltung über GPO ... 77
Überwachung ... ***77***
Systemmonitor ... **77**
Zuverlässigkeitsüberwachung/RACAgent ... **77**
Sammlungssätze ... **78**
Network Monitor ... **78**
Verwalten von Dateien ... ***78***
W2k8-Server Rolle: Dateidienste ... **78**
NTFS ... **78**
NTFS-Dateiberechtigung ... 78
NTFS-Encryption ... 78
Encrypting File System (EFS) ... **78**
File Replication Services (FRS) ... **78**
Distributed File System (DFS) ... **79**
Freigeben von Ordnern ... **79**
Schattenkopien ... **79**

Drucker *79*
Druckerpool konfigurieren **80**
Internetdrucken **80**
Migrieren von Drucker **80**
Verwalten von Druckern mit Skript **80**
IIS - Internet-Information-Server *80*
Lokales Dienstkonto 80
Netzwerkdienstkonto 80
Lokales Systemkonto 81
IIS installieren **81**
IIS Verwalten **82**
MS Office SharePoint *83*
BizTalk Server 2006 ..... *83*
Internet Secutity & Acceleration Server 2006 ..... *83*
Abkürzungen *84*
Abbildungsverzeichnis *85*
Index *86*

Einführung

Literatur: 70-640 Konfigurieren von Windows Server 2008 Active Directory
(MS Press / Dan Holme, Nelson Ruest, Danielle Ruest)
70-642 Konfigurieren einer Windows Server 2008 Netzwerkinfrastruktur
(MS Press / Tony Northrup)
70-643 Konfigurieren einer Windows Server 2008 Anwendungsplattform
(MS Press / J.C. Mackin, Anil Desai)

Links:

TOOLS

adaminstall.exe	AD LDS
adamsync.exe	AD LDS
adamuninstall.exe	AD LDS
adschemaanalyzer.exe	AD LDS
adsiedit.msc	
adprep	
adprep /domain	
adprep /domainprep /gpprep	
adprep /rodcprep	RODC einrichten
adprep /forestprep	
auditpol.exe	Überwachung von Verzeichnisdiensteinträgen
bcedit.exe	Start- und Wiederherstellungsmodus steuern
certutil.exe	Zertifikatdienst –Utility
convert	
convert /FS:NTFS	
Dcpromo.exe	
dcpromo /unattend	
dcpromo /adv	Wird weiterhin unterstützt
dcpromo /ApplicationPartitionsToReplicate	
dfsradmin.exe	Verwaltung der Replikation
dfsrmig.exe	Konfigurieren der DFS-R Replikation
diskpart.exe	Basic-Disks in Dynamic Disks konvertieren
dnscmd.exe	GNZ einrichten Anwendungsverzeichnispartitionen einrichten dnscmd /createdirectorypartition dnscmd /zoneexport Enable DNS Server to perform lookups in GlobalNames Zone dnscmd [server] /config /globalnamessupport 1
dnslint.exe	Diagnosetool für DNS
Dsacls.exe	Delegieren von Berechtigungen
Dsadd	
dsadd group	
dsamain.exe	Datenbankbereitstellungstool (LDAP)
dsdmgmt.exe	
dsdbutil.exe	Sichern von AD LDS-Instanzen
Dsfcmd.exe	
Dsget	Attribute eines Objektes abrufen
dsget user	
dsget group	
dsmgmt.exe	AD LDS
Dsmod	

dsmod user	
dsmod group	
Dsmove	
Dsquery	
dsquery user	
Dsrm	
Dnscmd.exe	
dnscmd /createdirectorypartitions	
dnscmd /ZoneExport	
gpmc.exe	Group Policy Administratror
Gpotool.exe	Prüfen der Gruppenrichtlinien
Gpresult.exe	Gruppenrichtlinienergebnissatz (RsOP)
Gpupdate.exe	Gruppenrichtlinienaktualisierung steuern
ipconfig	Diagnosetool
ipconfig /flushdns	DNS-Cache leeren
ldp.exe	Gelöschte AD-Objekte wiederherstellen Zertifikate testen
Mmc.exe	Microsoft Management Console
Netdom.exe	Computer zu Domäne hinzufügen. Vertrauensstellungen bearbeiten/prüfen
netdom renamecomputer %ComputerName% /newname:<ServerNeu> /reboot	
netdom join %ComputerName% /domain:contoso.com /userd: ContosoAdmin /password:*	
nlbmgr	NLB einrichten.
Nltest.exe	
ntdsutil.exe	
ntdsutil restore database	Authoritative Restore of AD DS überschreibt mit der restorten Datenbank alle anderen DCs Datenbanken.
ntdsutil set dsrm password	Zurücksetzen des DSRM-Passwortes
ntdsutil …	Application Directory Partitions erstellen
Oclist.exe	
Ocsetup.exe	
Oobe.exe	
oscdimg	Erstellt eine ISO-Datei
repadmin.exe	
repadmin /syncall	Zonentransfer forcieren
scregedit.wsf	Aktivieren von Remotedesktop
scw.exe	
scwcmd.exe	Sicherheitsrichtlinien in GPOs konvertieren
secedit.exe	Erstellen von Sicherheitsvorlagen
shutdown	
shutdown /r /t 0	Neustart des Computers einleiten
slmgr	
slmgr.vbs	Aktivieren von Windows-Server/MAK etc.
ultrasound.exe	Untersuchen und Beheben von Problemen mit der Replikation
w32tm.exe	Windows Zeitdienst
wbadmin.exe	Systemsicherung
wecutil	
wecutil qc	
winrm	
winrm quickconfig	
wlbs.exe	NLB control program

PowerShell

Windows PowerShell ist als Feature von W2k8 installiert, muss aber über Features hinzugefügt werden.

PowerShell verfügt über 130 **Befehlszeilenprogramme** (**Cmdlets**, "Command Lets").

Die Dateiendung bei Skripts lautet: ***.psl**

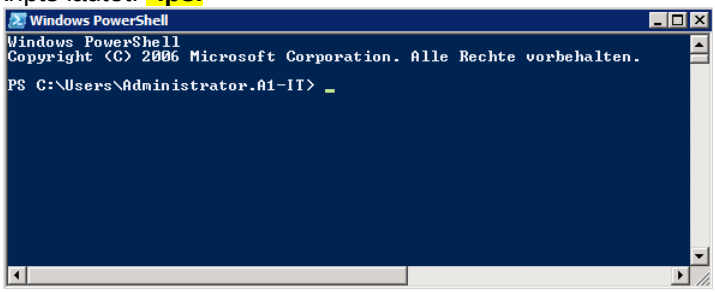


Abbildung 1: PowerShell

```
get-service
get-service | format-list

set-executionpolicy remotesigned
```

Beispiel: Benutzerimport.psl

```
$objOU=[ADSI]"LDAP://OU=People,DC=contoso,DC=com"
$dataSource=import-csv "NewUsers.csv"
foreach($dataRecord in $dataSource) {
   #Variablen zuweisen
   $cn=$dataRecord.cn
   …

   #Benutzerobjekt erstellen
   $objUser=$objOU.Create("user","CN="+$cn)
   $objUser.Put("sAMAccountName",$ sAMAccountName)
   …
   $objUser.SetInfo()
}
```

VBScript

Windows 2008 Core Installation

Bei der Installation von Windows Server 2008 handelt es sich wie bei Windows Vista um eine imagebasierte Installation. Daher nimmt das Installationsverfahren deutlich weniger Zeit in Anspruch als bei Vorgängerversionen von Windows.

Eine Server Core Installation kann das Angriffsrisiko verringern, da weniger Dienste installiert werden. Es werden weniger Updates benötigt, was den Verwaltungsaufwand verringert.

Server Core unterstützt 9 Serverrollen:

- Active Directory-Domänendienst
- Active Directory Lightweight Directory Services (AD LDS)
- DHCP-Server
- DNS-Server
- Dateidienste
- Druckserver
- Streaming Media-Dienste
- Webserver (IIS als statischer Webserver ASP.NET)
- Hyper-V (Windows Server-Virtualisierung)

Server Core unterstützt folgende 11 optionale Features:

- MS-Failovercluster
- Netzwerklastenausgleich
- Subsystem für UNIX-basierte Anwendungen
- Windows-Sicherung
- Multipfad-E/A
- Wechselmedienverwaltung
- Windows Bitlocker-Lauferkverschlüsselung
- Simple Network Management-Protokoll (SNMP)
- Windows Internet Name Service (WINS)
- Telnet-Client
- Quality of Service (QoS)

Installieren von Server Core

```
start /w ocsetup DHCPServerCore
net start dhcpserver
sc config dhcpserver start=auto
netsh interface ipv4 set address "LAN-Verbindung" dhcp
netsh interface ipv4 set dnsserver "LAN-Verbindung" dhcp

net user administrator *             // Ändern des Administratorkennwortes
```

Installieren eines Domänencontrollers

Da **Domänencontroller** wichtig für die **Authentifizierung** sind, sollten stets **mindestens zwei** in jeder Domäne Ihrer **Gesamtstruktur** betrieben werden, um für Fehlertoleranz zu sorgen.

Die Installation über die **Windows-Benutzeroberfläche** erfolgt in zwei Hauptschritten:

1. Die **Rolle AD DS** muss installiert werden

2. Die **AD DS** muss **installiert** und **konfiguriert** werden
   dcpromo.exe
   Installieren von ***Active Directory-Domänendiensten***

Schema
Unter **Schema** ist die Definition der **Attribute** und **Objektklassen** zu verstehen, die in einer Domäne vorhanden sein können.

Gesamtstruktur

Eine **Gesamtstruktur** ist eine Instanz in Active Directory.

Die **Gesamtstrukturstammdomäne** ist die **erste Domäne in der Gesamtstruktur**. Der einzige Zweck einer **dedizierten Gesamtrukturstammdomäne** ist die **Verwaltung der Infrastruktur der Gesamtstruktur**. Sie enthält standardmässig die **Einzelmastervorgänge** für die Gesamtstruktur. Ausserdem enthält sie besonders sicherheitskritische Gruppen wie **Organisations-Admins** und **Schema-Admins**, die weit reichende Auswirkungen auf die Gesamtstruktur haben können.

Die Theorie war, dass die dedizierte Gesamtstrukturstammdomäne die Sicherheit rund um diese gesamtstrukturweiten Funktionen verbessern würden. Nach den ersten Empfehlungen befände sich unterhalb der **dedizierten Gesamtstrukturstammdomäne** eine **einzelne globale untergeordnete Domäne** mit allen Objekten, die zu einer Domäne gehören: Benutzer, Gruppen, Computer etc. Siehe Abbildung

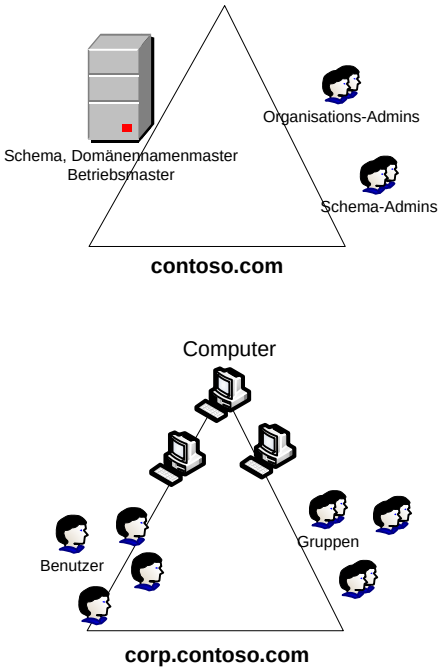


Abbildung 2: Beispiel einer Gesamtstrukturstammdomäne

Für die meisten Unternehmen ist es nicht länger empfehlenswert, eine dedizierte Gesamtstrukturstammdomäne zu implementieren. Die häufigste Empfehlung ist eine Gesamtstruktur mit einer einzigen Domäne.

Begründung:

- Mit jeder Gesamtstruktur mit mehreren Domänen sind Risiken und Kostenverbunden.
- Es gibt noch keine Tools, die einem Unternehmen das Löschen und Einfügen von Active Directory-Strukturen ermöglichen.
- Innerhalb einer einzigen Domäne können Sie die Sicherheit der geringsten Rechte implementieren, was mindestens genauso sicher ist, wenn nicht sicherer ist als eine dedizierte Gesamtstrukturstammdomäne mit einer untergeordneten Domäne.

Sie sollten niemals eine Gesamtstruktur mit mehreren Domänen erstellen, nur um die organisatorische Struktur Ihres Unternehmens wiederzuspiegeln. Stattdessen sollte Ihr Domänenmodell von den Eigenschaften der Domänen selbst abgeleitet werden.

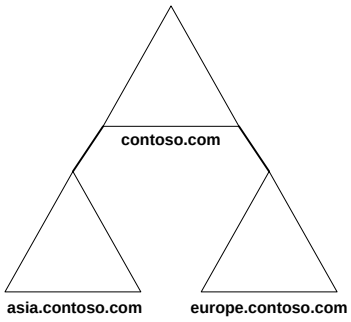


Abbildung 3: Gesamtstruktur mit einer einzigen Struktur

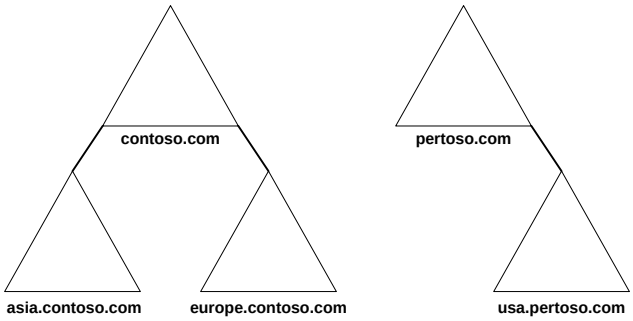


Abbildung 4: Gesamtstruktur mit mehreren Strukturen

Active Directory-Migrationstoll (ADMT)

Das **Active Directory-Migrationstool**, Version 3(ADMT v3), kann Aufgaben zur **Objektmigration** und **Sicherheitskonvertierung** durchführen.
Mithilfe von **ADMT** können Sie Objekte zwischen einer **Quell-** und einer **Zieldomäne** migrieren.
Bei der Durchführung der Migrationsaufgaben gibt **ADMT** Ihnen die Möglichkeit, die **Migration zu simulieren**.

Folgende Komponenten sind bei einer Migration wichtig:

- Local Security Authority Subsystem (LSASS)
- sIDHistory
- Sicherheitskonvertierung
- Kennwortmigration
- Dienstkonten
- Nicht migrierbare Objekte

Installieren einer neuen W2k8-Gesamtstruktur

Heraufstufen des Servers mit:

- **dcpromo.exe /unattend:"Pfad der Antwortdatei"**
  DNS-Name ➔
  NetBIOS-Name ➔

Beim Erstellen einer neuen **Stammdomäne** der **Gesamtstruktur** müssen Sie deren **DNS-Namen** (Domain Name System), ihren **NetBIOS-Namen** sowie die Gesamtstruktur- und Domänenfunktionsebenen angeben.

Der erste **Domänencontroller** darf kein schreibgeschützter Domänencontroller, sondern muss ein **globaler Katalogserver** sein.

Installieren weiterer Domänencontroller in einer Domäne

Wenn der Gesamtstruktur Domänencontroller kein W2k8-Server ist muss die Umgebung vorbereitet werden.

1. Anmelden am **Schemamaster**
2. **<W2k8-DVD>:\Sources\Adprep*.*** ➔ auf den **Schemamaster** kopieren
3. **adprep /forestprep**
4. **adprep /rodcprep**
5. **adprep /domainprep /gpprep**

Weitere **Domänencontroller** können hinzugefügt werden, indem die **AD DS** installiert wird.
Auswählen der Bereitstellungskonfiguration
Eingeben der Sicherheitsinformationen für das Netzwerk

Auswählen der Domäne und des Standorts
Optionen konfigurieren: DNS-Server, globaler Katalogserver oder RODC

Installieren einer neuen untergeordneten W2k8-Server-Domäne

1. adprep /forestprep
2. Installieren der AD DS (dcpromo)
3. Option: Neue Domäne in vorhandener Gesamtstruktur erstellen
4. Option: Neue untergeordnete Domäne erstellen

Installieren einer neuen Domänenstruktur

Zusätzliche Strukturen sind weitere Domänen, die sich nicht im selben **Namespace** befinden.

Strukturen in einem Namespace!

contoso.com
subsidiary.contoso.com

Strukturen in verschiedenen Namespaces!

contoso.com
tailspintoys.com

1. adprep /forestprep
2. Installieren der AD DS (dcpromo) / erweiterten Modus verwenden
3. Option: Neue Domäne in vorhandener Gesamtstruktur erstellen
4. Option: Neuen Domänenstrukturstamm erstellen

Installation eines RODC für Zweigstellen

Voraussetzungen
Der Server muss Mitglied einer **Arbeitsgruppe** und **nicht der Domäne** sein!

Die Installation erfolgt in zwei Phasen:

1. **Erstellen des Kontos des schreibgeschützten Domänencontrollers**
   OU: Domänencontroller
   Konto für schreibgeschützten Domänencontroller vorbereiten
   Delegieren einer Gruppe oder eines Benutzers zur Verwaltung
   (Verfügt nach der Installation über lokale Administratorenrechte auf dem Server)

2. **Zuordnen des Servers zum Konto des schreibgeschützten Domänencontrollers**
   dcpromo /useexistingaccount:attach

Installieren der AD DS von einem Medium

Die **AD DS** lässt sich über die Option: ***Installieren von Medium*** effizienter installieren.
Damit lassen sich Auswirkungen auf die **Netzbandbreite** zeitlich steuern.

1. Erstellen von Installationsmedien auf einem **beschreibbaren W2k8-Server**
   Nur Installationsdateien oder inkl. **SYSVOL**
2. **ntdsutil**
   activate instance ntds

ifm

Optional:
create sysvol full <Pfad>
create full <Pfad>
create sysvol rodc <Pfad>
create rodc <Pfad>

Entfernen eines Domänencontrollers

Zum entfernen eines Domänencontrollers verwenden Sie den Befehl: **dcpromo.exe**

Falls während des herabstufen des Domänencontrollers **keine Verbindung zur Domäne** besteht, können Sie: **dcpromo /forceremoval** verwenden.

Konfigurieren von Betriebsmastern

In einer **Active Directory-Domäne** sind **alle Domänencontroller gleichbedeutend**. Doch bei der **Multimaster-Replikationstopologie** dürfen verschiedene Vorgänge von nur einem System durchgeführt werden. Deshalb sind in einer Active Directory-Domäne **Betriebsmaster**, **Domänencontroller mit bestimmten Rollen**.
Die **Betriebsmaster-Rollen** werden auch **Token** genannt. Die Rollen können an andere Server weitergegeben werden ohne das ein Neustart des System notwendig ist.

Die Grundidee ist:

Ein Domänencontroller führt die Aufgabe aus, und in diesem Zeitraum führt kein anderer Domänencontroller dieselbe Aufgabe aus!

Es gibt **fünf Betriebsmaster-Rollen**. Zwei für die **Gesamstruktur** und drei pro **Domäne**.
In einer **Gesamtstruktur** mit **zwei Domänen** gibt es also acht Betriebsmaster (2 + 2*3).

Flexible Single Master Operations (FSMOs)

Betriebsmaster-Rollen für die Gesamtstruktur:

- **Domänenname**
- **Schema**

Betriebsmaster-Rollen pro Domäne:

- **RID**
- **Infrastruktur**
- **PDC-Emulator**

Welcher **Server** die **Domänennamen-Rolle** innehat, kann mit dem **Snap-In:** ***Active Directory-Domänen und Vertrauensstellungen*** geprüft werden.

Abbildung 5: Betriebsmaster Gesamtstruktur

Welcher **Server** die **Schemamaster-Rolle** innehat, kann mit dem **Snap-In:** ***Active Directory-Schema*** geprüft werden.
➔ Dieses Snap-In muss zuerst registriert werden! **regsvr32 schmmgmt.dll**

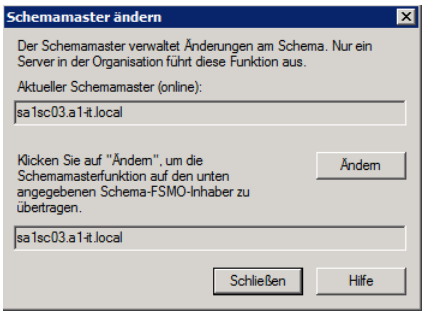


Abbildung 6: Betriebsmaster Schema

Welche **Server** welche **Domänen-Rollen** innehaben, kann mit dem **Snap-In:** ***Active Directory-Benutzer und Computer*** geprüft werden.

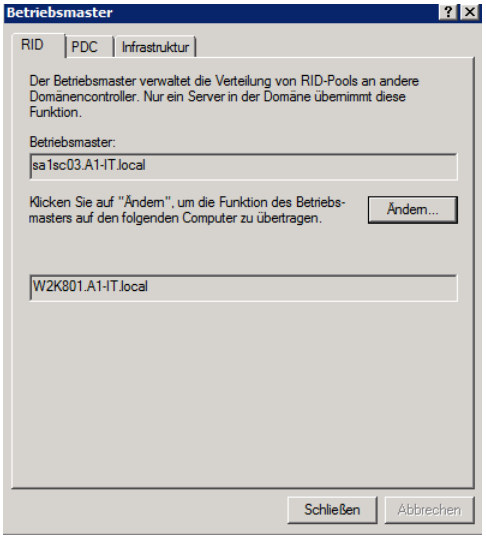


Abbildung 7: Betriebsmaster Domäne

Domänennamenmaster

Der Domänennamenmaster kommt beim **Hinzufügen und Entfernen von Domänen in der Gesamstruktur** zum Einsatz.

Beim Ausfall des Domänennamenmasters können keine Änderungen an der Domäne vorgenommen werden.

Diese Rolle kann nach einer Übernahme nicht mehr an den ursprünglichen Master zurückübertragen werden. Der ursprüngliche Master muss vollständig ausser Betrieb gesetzt werden. Physisch vom Netz nehmen und die AD DS mit dcpromo /forceremoval entfernen!

Schemamaster

Der Domänencontroller mit der Schemamaster-Rolle ist für Änderungen am Schema der Gesamtstruktur zuständig. Wenn Sie das Schema ändern oder eine Anwendung installieren möchten, die das Schema ändert, sollten Sie dies auf dem Domänencontroller mit der Schemamaster-Rolle ausführen.

Der Ausfall am Schemamaster hindert Sie nur an Änderungen am Schema.

Diese Rolle kann nach einer Übernahme nicht mehr an den ursprünglichen Master zurückübertragen werden. Der ursprüngliche Master muss vollständig ausser Betrieb gesetzt werden. Physisch vom Netz nehmen und die AD DS mit dcpromo /forceremoval entfernen!

RID-Master

Der **RID-Master** spielt eine wichtige Rolle bei der Generierung von **Sicherheitskennungen** (SIDs) für Sicherheitsprinzipale wie Benutzer, Gruppen und Computer. Die SID eines Sicherheitsprinzipales muss eindeutig sein.

Die **RID-Master-Rolle** kann mit der Funktion eines **DHCP für SIDs** verglichen werden.

Der Ausfall des RID-Masters hindert Domänencontroller letzlich am Erstellen neuer SIDs und demzufolge am Erstellen neuer Konten für Benutzer, Gruppen und Computern.

Diese Rolle kann nach einer Übernahme nicht mehr an den ursprünglichen Master zurückübertragen werden. Der ursprüngliche Master muss vollständig ausser Betrieb gesetzt werden. Physisch vom Netz nehmen und die AD DS mit dcpromo /forceremoval entfernen!

Infrastrukturmaster

In einer Umgebung mit mehreren Domänen ist es normal, dass ein Objekt auf Objekte in anderen Domänen verweist. Sie können sich den Infrastrukturmaster als Kontrollgerät für Gruppenmitgliedschaften aus anderen Domänen vorstellen.

Ein Ausfall des Infrastrukturmasters fällt nur Administratoren, nicht aber Benutzern auf.

Diese Rolle kann nach einer Übernahme an den ursprünglichen Master zurückübertragen werden.

Phantomobjekt

Wenn Sie ein Mitglied aus seiner anderen Domäne einer Gruppe in Ihrer Domäne hinzufügen, wird das Attribut ***member*** der Gruppe an den definierten Namen des neuen Mitglieds angefügt. Ihre Domäne hat jedoch ggf. nicht immer Zugriff auf einen Domänencontroller in der Domäne des Mitglieds, weshalb Active Directory zum Abbilden des Mitglieds ein **Phantomobjekt** erzeugt. Das **Phantomobjekt** enthält nur die **SID**, den definierten Namen (**DN**) und die **GUID** des Mitglieds.

PDC-Emulator

Stellt eine **wichtige Aufgabe** in der Domäne dar!

Der Ausfall eines PDC-Emulators wirkt sich am unmittelbarsten auf den Betrieb aus!

Diese Rolle kann nach einer Übernahme an den ursprünglichen Master zurückübertragen werden.

- **Emuliert einen primären Domänencontroller (PDC) zum Zweck der Abwärtskompatibilität dar.**
  Für ältere Tools, Dienstprogramme und Clients welche einen PDC erwarten.

- **Nimmt an einer besonderen Kennwortaktualisierungsverarbeitung für die Domäne teil.**
  Änderungen an einem Kennwort werden sofort an den PDC weitergeleitet. Wird ein Anmeldeversuch abgelehnt wird sofort ein Authentifizierungsversuch an den PDC gesendet. Auf den PDC sollten deshalb alle Clients Zugriff haben. Der PDC sollte zuverlässige Verbindung und hohe Leistung haben.

- **Verwaltet Gruppenrichtlinienaktualisierungen innerhalb der Domäne.**

- **Stellt eine zentrale Zeitquelle für die Domäne bereit.**
  Stellt sicher das der **Zeitstempel** für: Active Directory, Kerberos, FRS und DFS-R synchron sind. Alle anderen Domänencontroller in der Domäne synchronisieren sich mit dem PDC über den

Dienst **Win32Time** mit der **UTC**-Zeit.
Der **PDC** selbst kann sich mit einer externen Zeitquelle synchronisieren.

- **Fungiert als Hauptsuchdienst der Domäne**

Platzieren von Betriebsmastern

Domänennamenmaster und **Schemamaster** auf einem Server.
- Die Last dieser Betriebsmaster-Rollen ist sehr gering.

PDC-Emulator und **RID-Master** auf einem Server
- Auf zuverlässige Verbindung und hohe Leistung achten.

Infrastrukturmaster auf einem Server der ***kein globaler Katalogserver*** ist

Übertragen von Betriebsmaster-Rollen

Wenn Sie einen Domänencontroller offline oder ausser Betrieb schalten möchten, der gegenwärtig eine Betriebsmaster-Rolle innehat, müssen Sie diese Rolle vorher an einen anderen Domänencontroller übertragen.
Wenn ein Server ausfällt können Sie die Rolle auch übernehmen, was aber eine drastische Massnahme ist.

Vorgehen:
1. Verbinden Sie sich mit dem Domänencontroller, an den Sie die Rolle übertragen möchten.
2. Öffnen Sie das Snap-In und ändern Sie den Server.

Zum übernehmen von Rollen kann auch das **Verwaltungstool *ntdsutil*** eingesetzt werden.

Funktionsebenen

Funktionsebenen sind wie Schalter, die neuen Funktionen aktivieren, die von der jeweiligen Windows-Version bereitgestellt werden. **Diese Funktionen sind nicht abwärtskompatibel**. Die Verbesserungen an der Verwaltung der AD DS können Sie erst nutzen, wenn auf allen **DCs W2k8-Server** ausgeführt wird.

Die Funktionsebenen betreffen nicht Mitgliedserver und Arbeitsstationen.

Domänenfunktionsebenen

Snap-In: ***Active Directory-Domänen und –Vertrauensstellungen***

Die Domänenfunktionsebene bestimmt die Active Directory-Funktionen, die innerhalb der Domäne zur Verfügung stehen, und legt die Windows-Versionen fest, die für die Domänencontroller innerhalb einer Domäne unterstützt werden.

- **Windows 2000 einheitlich**
- **Windows Server 2003**
  - Umbenennen von DC's
  - Attribut: lastLogonTimestamp
  - Attribut: userPassword
  - Umleitung der Standardcontainer für Benutzer und Computer
  - Richtlinien des Authorisierungs-Managers
  - Eingeschränkte Delegierung
  - Ausgewählte Authentifizierung
- **Windows Server 2008**
  - DFS-R von SYSVOL
  - Advanced Encryption Services (AES)
  - Letzte interaktive Anmeldeinformation

- Fein abgestimmte Kennwortrichtlinien
  (Fine-grained password policy)

Wenn Sie Domänenfunktionsebenen hochstufen, werden neue Funktionen von Active Directory aktiviert.

Gesamtstrukturfunktionsebenen

Snap-In: ***Active Directory-Domänen und –Vertrauensstellungen***

Gesamtstrukturfunktionsebenen ermöglichen Funktionen in der Gesamtstruktur und legen die Betriebssystem fest, die für DCs in der gesamten Gesamtstruktur unterstützt werden.

- **Windows 2000 einheitlich**
- **Windows Server 2003**
  - Gesamtstrukturvertrauensstellungen
  - Domänenumbenennung
  - Replikation verknüpfter Werte
  - Unterstützung für **RODCs**
  - Verbesserte **KCC-Algorithmen** und Slalierbarkeit
  - Konvertierung von **inetOrgPerson ←→ user-Objekt**
  - Unterstützung für die Erweiterungsklasse **dynamicObject**
  - Unterstützung für Anwendungsgruppen und LDAP-Abfragegruppen
  - Deaktivierung und Neudefinition von Attributen und Objektklassen
- **Windows Server 2008**

Konfigurieren der DFS-Replikation von SYSVOL

SYSVOL ist ein Ordner im Verzeichnis **%SystemRoot%\SYSVOL** und enthält **Anmeldeskripts**, **Gruppenrichtlinienvorlagen** und **andere Ressourcen**, die für die **zuverlässige Verwaltung einer Active Directory-Domäne** sehr wichtig sind.

Sie müssen sicherstellen, dass alle Änderungen in **SYSVOL** auf alle Domänencontroller repliziert werden. Vor **W2k8-Server** geschah das mit dem **Dateireplikationsdienst** (File Replication Service, FRS). FRS hat Einschränkungen bezüglich **Kapazität** und **Leistung** und ist recht **kompliziert** zu installieren. Mit W28-Server können Sie **DFS-R** zur Replikation von **SYSVOL** verwenden.

Achtung der Replikationsintervall beträgt bis zu 15 Minuten!

Die Migration von FRS nach DFS-R erfolgt in mehreren Phasen:

1. Hochstufen der Gesamtstruktur Domänenfunktionsebene auf "Windows Server 2008"
2. Status prüfen: **dfsrmig /getglobalstate**
3. Phase 0(Starten): **dfsrmig /setglobalstate 0**
4. Status prüfen: **dfsrmig /getglobalstate**
   Muss Erfolgreich sein!
5. Phase 1(Vorbereiten): **dfsrmig /setglobalstate 1**
6. Status prüfen: **dfsrmig /getglobalstate**
   Muss Erfolgreich sein! Alle Domänencontroller konsistent.
7. Phase 2(Umleiten): **dfsrmig /setglobalstate 2**
8. Status prüfen: **dfsrmig /getglobalstate**
   Muss Erfolgreich sein! Alle Domänencontroller konsistent.
9. SYSVOL prüfen: **net share**
   Die Freigabe von NETLOGON muss auf den Ordner **SYSVOL_DFSR** verweisen!
10. Phase 3(Entfernt): **dfsrmig /setglobalstate 3**
11. Status prüfen: **dfsrmig /getglobalstate**
    Muss Erfolgreich sein! Status Entfernt.

Standorte und Replikation

Als Administrator eines auf Windows basierenden Netzwerkes besteht eine Ihrer Aufgaben darin, eine möglichst effiziente Authentifizierung und eine optimale Replikation zwischen Domänencontrollern sicherzustellen. Insbesondere wenn Ihr Netzwerk über teure und langsame Leitungen verfügt.

Konfigurieren von Standorten und Subnetzen

Die Netzwerktopologie wird durch Objekte namens Standorte und Subnetze representiert.

Standortobjekte werden verwendet um die **Replikation** und die **Dienstlokalisierung** zu steuern.

Replikationsdatenverkehr

Mit der Steuerung des Replikationsdatenverkehrs können Replikationen zeitlich gesteuert und geplant werden.

Dienstlokalisierung (SRV-Einträge)

Wenn Sie mehrere Netzwerkstandorte und an jedem einen Domänencontroller verwalten, sollte die **Authentifizierung der Clients** am Domänencontroller des jeweiligen Standortes erfolgen. Dies ist ein Beispiel für Dienstlokalisierung.
Andere Dienste können ebenfalls lokalisiert werden. DFS-Namespaces sind beispielsweise ein lokalisierter Dienst.
Wenn ein Domänencontroller hinzugefügt wird, kündigt dieser seine Dienste durch Erstellen von **SRV-Einträgen** (Service Locator) im DNS an.
Folgende Dienste werden eingetragen:

Authentifizierungs- und Verzeichnisdienste	**Port: 3268**
Kerberos	**Port: 88**
LDAP	**Port: 389**

Standorte erstellen

Snap-In Active Directory-Standort und –Dienste.
Es empfiehlt sich die Standortnamen gezielt anzupassen, damit sie die Geschäfts- und Netzwerktopologie reflektiert.

Ein Standort kann mit mehreren Subnetzen verknüpft sein!

Subnetzobjekt

Ein Subnetzobjekt definiert einen Bereich von IP-Adressen und ist mit einem Standort verknüpft. Die Standardstandortverknüpfung ist **DEFAULTIPSITELINK**.
Standorte sind dann sinnvoll wenn der Client oder Server den Standort kennt, zu dem er gehört. Dies wird normalerweise erreicht, indem die **IP-Adresse** des Systems mit einem Standort verknüpft wird, und Subnetzobjekte leisten diese Verknüpfung.

Eins Subnetz kann mit nur einem Standort verknüpft werden!

Achtung! VPN-Adressbereiche nicht vergessen!

Globaler Katalog und Anwendungsverzeichnispartition

Die **AD DS** ist ein **Datenspeicher** für die Identitäts- und Zugriffsverwaltung. Die **Verzeichnisdatenbank** ist **ntds.dit**. Innerhalb dieser einzelnen Datei befinden sich **Verzeichnispartitionen**. Jede Verzeichnispartition, die auch als **Namenskontext** (NC) bezeichnet wird, enthält Objekte mit einem bestimmten Funktionsumfang und Zweck. Drei wichtige **Namenskontexte** sind:

- **Domäne-NC**
- **Konfiguration-NC**
- **Schema-NC**

Der Domänennamenskontext für eine Domäne wird auf alle Domänencontroller innerhalb einer Domäne, jedoch nicht auf Domänencontroller in anderen Domänen repliziert, sodass **jeder Domänencontroller** mindestens drei Replikate besitzt: **Domäne-NC, Konfiguration-NC, Schema-NC**.

Bei den **RODCs** wird neu nicht eine vollständige Kopie der NCs gespeichert. Vertrauliche Daten wie Benutzerkennwörter werden hier nicht gespeichert.

Globaler Katalog (Global Catalog, GC)

Teilattributsatz (Partial Attribute Set, PAS)

Beim Erstellen der ersten Domäne in der Gesamtstruktur wird der ***erste Domänencontroller als GC*** konfiguriert. Für jeden weiteren DC müssen Sie entscheiden, ob er als GC-Server dienen soll.
➔ NTDS Settings

Was geschieht, wenn ein Benutzer in Domäne B nach einem Benutzer, Computer oder einer Gruppe in Domäne A sucht? Die Domänencontroller in Domäne B verwalten keine Informationen über Objekte in Domäne A. Ein Domänencontroller in Domäne B könnte daher keine Anfrage zu Objekten im Domänen – NC der Domäne A beantworten.

Hier kommt der **globale Katalog** (GC) ins Spiel. Der **globale Katalog** ist eine **Partition**, in der Informationen zu jedem Objekt in der **Gesamtstruktur** abgelegt sind. Wenn ein Benutzer in **Domäne B** nach einem Objekt in **Domäne A** sucht, stellt der **GC** die Ergebnisse der Abfrage bereit. Um die Effizienz des **GC** zu optimieren, enthält er nicht jedes Attribut zu jedem Objekt in der Gesamtstruktur. Stattdessen umfasst er eine **Teilmenge** von Attributen, die für die domänenübergreifende Suche hilfreich sind. Daher wird der GC auch als **Teilattributsatz** (Partial Attribute Set, PAS) bezeichnet. Was seine Suchfunktion betrifft, so können Sie sich den **GC** als eine **Art Index** für den **AD DS-Datenspeicher** vorstellen.

Idealerweise wäre jeder Domänencontroller ein GC-Server.

Universelle Gruppenmitgliedschaft (UGMC)

Universal Group Membership Caching (UGMC)

Snap-In: ***Active Directory-Standorte und –Dienste (NTDS Site Settings)***

Universelle Gruppen enthalten Benutzer und Gruppen aus mehreren Domänen in einer Gesamtstruktur. Die Mitgliedschaft in universellen Gruppen wird im GC repliziert.
Ist kein GC-Server verfügbar, sind Benutzer effektiv nicht in der Lage, sich anzumelden und auf Netzwerkressourcen zuzugreifen.
Dient jeder Domänencontroller als GC-Server, wird dieses Problem nicht auftreten. Um eine erfolgreiche Anmeldung zu erleichtern, können Sie die Zwischenspeicherung der **universellen Gruppenmitgliedschaft** (Universal Group Membership Caching, UGMC) ermöglichen.

In **Standorten** mit **unzuverlässigen Verbindungen** und **ohne eigenen GC-Server** empfiehlt es sich auf dem Domänencontroller **UGMC** zu konfigurieren.

Anwendungsverzeichnispartitionen

Anzeigen: ***ADSI-Editor***
Bearbeiten: ***ntdsutil.exe, ldp.exe (*Organisations-Admins)**

Eine Anwendungsverzeichnispartition ist ein Teil des Datenspeichers, der Objekte enthält, die von einer Anwendung oder einem Dienst ausserhalb des Haupt-AD DS-Dienstes benötigt werden. Im Gegensatz zu anderen Partitionen können Anwendungspartitionen gezielt auf bestimmte Domänencontroller repliziert werden. Sie werden nicht standardmässig auf alle DCs repliziert.
Anwendungsverzeichnispartitionen sind auf die Unterstützung verzeichnisfähiger Anwendungen und Dienste ausgerichtet.

DNS ist ein Dienst der mit **Anwendungsverzeichnispartitionen** arbeitet. Die Partitionen des DNS werden nur auf Domänencontroller repliziert welche als DNS-Server fungieren. **TAPI** ist ebenfalls ein solcher Dienst.

Im Allgemeinen werden Sie spezielle Anwendungstools verwenden, um die Anwendungsverzeichnispartitionen, die zugehörigen Daten und die Replikation zu verwalten.

Vor dem Herabstufen eines Domänencontrollers sollten Sie unbedingt die Anwendungsverzeichnispartitionen untersuchen und bewerten. Beim herabstufen des DC gehen alle Informationen in der Partition verloren.

Konfigurieren der Replikation

Was Sie sich im Zusammenhang mit der **Active Directory-Replikation** merken müssen ist, dass sie so aufgebaut sein muss, dass letztlich **jedes Replikat** auf einem Domänencontroller mit den Replikaten der jeweiligen Partition konsistent sein muss, die auf anderen Domänencontrollern gehostet wird.

Die Active Directory-Replikation stellt sicher, dass alle Änderungen an einer Partition auf alle Replikate der Partition übertragen werden. Die Active Directory-Replikation

- Integrität und Konsistenz durch lose Kopplung.
- Effektive bidirektionale Replikationstopologie
- Konflikterkennung und –verwaltung

Verbindungsobjekte

Snap-In: ***Active Directory-Standorte und –Dienste(NTDS Settings)***

Ein Domänencontroller repliziert Änderungen von einem anderen Domänencontroller aufgrund von **AD DS-Verbindungsobjekten**, die auch einfach als **Verbindungsobjekte** bezeichnet werden. Verbindungsobjekte sind **unidirektional** und arbeiten mit der **Pulltechnologie**.

Die Stellen werden als:
Downstreamreplikationspartner und **Upstreamreplikationspartner** betrachtet.

Konsistenzprüfung (KCC)

Knowledge Consistency Checker (KCC)

Die **Replikationstopologie** muss nicht manuell erstellt werden, standardmässig erstellt Active Directory eine effektive Replikationstopologie.
Die Topologie ist **bidirektional**, sodass die Replikation beim Ausfall eines Domänencontrollers ununterbrochen fortgesetzt wird. Die Topologie stellt ausserdem sicher, dass zwischen zwei beliebigen Domänencontrollern immer nur **drei Abschnitte (Hops)** liegen.
Die **KCC** analysiert die Domänencontroller in einem Standort und erstellt **Verbindungsobjekte**, um die oben beschriebene **bidirektionale Drei-Hop-Topologie** zu erstellen.
Wenn ein Domänencontroller einem Standort hinzugefügt oder daraus entfernt wird oder wenn ein Domänencontroller nicht reagiert, ordnet die **KCC** die Topologie dynamisch um und fügt Verbindungsobjekte hinzu bzw. löscht diese, um erneut eine effektive Replikationstopologie zu gewährleisten.
Sie können Verbindungsobjekte manuell erstellen und dauerhaft Replikationspfade festlegen.

Bei **KCC** Errors im Systemlog kann man auf Replikationserrors schliessen.

In **Disaster Rcovery** Überlegungen müssen **Standbybetriebsmaster** miteinbezogen werden.

Benachrichtigung

Benachrichtigung ist der Vorgang, durch den ein **Upstreampartner** seinen **Downstreampartner** mitteilt, dass eine Änderung verfügbar ist. Die Übertragung erfolgt durch den **Directory Replikation Agent** (DRA)

Die Änderungen werden in eine Warteschlange gestellt, die Benachrichtigung über die Änderung erfolgt innerhalb 15 Sekunden.

Abfragen (Polling)

Mit dem **Polling** überprüft der **Downstreampartner** ob sein **Upstreampartner** online ist und ob einfach keine Änderungen vorliegen.
Standardmässig ist das **Abfrageintervall** für die standortinterne Replikation **eine Stunde**.
Wenn ein **Upstreampartner** nicht auf wiederholte Abfragen reagiert, startet der **Downstreampartner** die **KCC**, um die Replikationstopologie zu überprüfen. Wenn der Upstreampartner tatsächlich offline ist, wird die **Replikationstopologie des Standorts neu erstellt**, um die Änderungen zu berücksichtigen.

Standortverknüpfungen

Standardmässig sind Standortverknüpfungen transitiv. Kann aber auch deaktiviert werden.

Es empfiehlt sich Standortverknüpfungen manuell zu erstellen, die der Topologie Ihres physischen Netzwerks entsprechen.

Standortverknüpfungsbrücken

Eine Standortverknüpfungsbrücke verbindet zwei oder mehr Standortverknüpfungen, so dass eine transitiver Verknüpfung entsteht. Standortverknüpfungsbrücken sind nur dann erforderlich, wenn Sie die Option Brücke zwischen allen Standortverknüpfungen herstellen für das Transportprotokoll deaktiviert haben.

Standortverknüpfungskosten

Sie können Standortverknüpfungskosten so konfigurieren, um darauf hinzuweisen, dass eine Verknüpfung schneller, zuverlässiger oder bevorzugter ist. Langsame Verbindungen verursachen höhere Kosten als schnelle Verbindungen. Active Directory repliziert über die Verbindung mit den niedrigsten Kosten.

Replikationsprotokolle

- **Directory Service Remote Procedure Call** (DS-RPC)

- **Inter-Site Messaging-Simple Mail Transport Protocol** (ISM-SMTP)

Replikationshäufigkeit

Die **standortübergreifende Replikation** basiert nur auf Abfragen, es gibt **keine Benachrichtigung**. Standardmässig fragt ein Bridgeheadserver **alle drei Stunden** seine **Upstreamreplikationspartner** ab, um festzustellen, ob Änderungen verfügbar sind.

Replikationzeitpläne

Standardmässig erfolgt die Replikation rund um die Uhr. Sie können die standortübergreifende Replikation jedoch auf bestimmte Tageszeiten beschränken.

Überwachen der Replikation

Repadmin.exe

Berichterstattung zum Replikationsstatus.
Mit repadmin.exe können Sie auch die Replikationstopologie erstellen und die Replikation erzwingen.

- Anzeigen der Replikationspartner für einen DC.
- Anzeigen von Verbindungsobjekten für einen DC
- Anzeigen von Metadaten zu einem Objekt
- Starten der KCC
- Erzwingen der Replikation zwischen zwei Partnern
- Synchronisieren eines DC mit allen Replikationspartnern

DSA_LIST ➔ Netzwerkbezeichnung (DNS- oder NetBIOS-Name)

Dcdiag.exe

- Tool for Domain Controller (DC/ADS) analysis/troubleshooting.
- Tool zur Verzeichnisdiagnose.
- Führt eine Reihe von Tests aus, und erstellt einen Bericht zum allgemeinen Status der Replikation und Sicherheit für AD DS.

Features:

- FrsEvent
- DFSREvent
- Intersite
- KccEvent
- Replications
- Topology
- Verify Replicas

Bridgeheadserver

Um die Replikation effizienter zu gestalten, wird ein Domänencontroller als **Bridgeheadserver** ausgewählt. Der **Bridgeheadserver** ist für die gesamten in einen Standort eingehenden und daraus ausgehenden **Replikationsvorgänge für eine Partition** zuständig. Ein **Bridgeheadserver** ist für die Replikation von Änderungen an einer Partition von anderen **Bridgeheadservern in anderen Standorten** verantwortlich.
Bridgeheadserver werden automatisch ausgewählt, und der **ISTG** erstellt die standortübergreifende Replikationstopologie so, dass Änderungen effektiv zwischen Bridgeheadservern repliziert werden, die eine Standortverknüpfung teilen. Bridgeheadserver werden pro Partition ausgewählt. Es ist daher möglich, dass ein DC in einem Standort der Bridgeheadserver für das Schema ist und ein anderer der für die Konfiguration.

Es können auch bevorzugte Bridgeheadserver definiert werden.
Generator für Standortübergreifende Topologie (Intersite Topology Generator, ISTG).

Business Continuity

Aufrechterhaltung des Geschäftsbetriebs durch proaktive Überwachung.

Das ausführen von **Microsoft Windows-Technologien** ohne **proaktive Überwachung** ist nicht ratsam!

Speichern Sie keine anderen Daten auf dem Domänencontroller!

Schützen Sie ihren DC mit dem **Volumeschattenkopie-Dienst** (VSS).

Aufgabenfrequenz: Täglich, wöchentlich, monatlich und ad hoc.

Die **IT** ist für die **Dienstverwaltung** zuständig und die **Benutzer** sind für die **Daten** zuständig.

Um **zuvor belegten Speicherplatz wiederherzustellen**, müssen Sie die **Datenbank offline** schalten und einer **Komprimierung** und **Defragementierung** unterziehen.

Unter **W2k8-Server** kann der **AD DS-Dienst** heruntergefahren und wieder gestartet werden. Damit Sie den AD DS-Dienst beenden können, muss der DC mit **einem anderen DC kommunizieren können**, auf dem der Dienst ausgeführt wird.

Acctinfo.dll

Um ***zusätzliche Kontoinformationen*** zu verwalten, können Sie die Datei **Acctinfo.dll** herunterladen und registrieren. Dieses DLL kann für Helpdeskmitarbeiter und Domänenadministratoren sehr hilfreich sein.

Registration: **regsvr32 acctinfo.dll**

- Domain PW Info
- SID History
- Set PW On Site DC

ALTools.exe

Account Lockout and Management Tools.
Speichern unter: ***Dokumente***

Specops Gpupdate

Kostenloses Zusatzprogramm.
www.specopssoft.com/products/specopsgpupdate/download.asp

- Remoteaktualisierungen von GPOs
- Remotestarts von Computern
- Remoteneustart- oder herunterfahren von Computern

Verzeichnisschutzmassnahmen

Wenn Sie ein Konto löschen, können Sie es anschliessend nicht einfach neu erstellen. Wenngleich das Konto dem menschlichen Auge identisch vorkommt, stellt es für die AD DS ein völlig anderes Objekt dar,

da es nicht die Attribute des zuvor gelöschten Objektes beibehält. Das ist ein guter Grund, ein Konto neu zuzuweisen, anstatt es neu zu erstellen, wenn Mitarbeiter ihren Standort im Netzwerk ändern.

Features zum Schutz der AD DS-Objekte:

- **Objektschutzoption** (Erweiterte Features)
  - Weist ***jeder*** zwei Berechtigungen zu.
- **AD DS-Zugriffsüberwachungsfunktion**
  - Wenn Sie unter W2k8-Server ***Verzeichnisänderungen*** überwachen, werden bei jeder Objektänderung ***alte und neue Werte protokolliert***.
- **Tombestonecontainer**
  - Objekte werden standardmässig **180 Tage** hier aufbewahrt.
- **Windows Server-Sicherung**
  - Beim wiederherstelle aus einer Sicherung werden **alle Attribute wiederhergestellt**.

Gelöschte Active Directory-Objekte könne mit dem Befehlszeilentool **ldp.exe** wiederhergestellt werden.

Quest Object Restore for Active Directory

Kostenloses Zusatzprogramm: www.quest.com/object-restore-for-active-directory

Object-Wiederherstellung aus dem **Tombstonecontainer**.

Windows Server-Sicherung

Ordner: WindowsImageBackup
File-Extension: .vhd-Datei
Datensicherungen werden im selben Format gespeichert wie die "Complete PC-Sicherung" von WVista.
Die Sicherungsdateien (vhd-Dateien) können mit ***VHDMount*** geladen werden.

Systemwiederherstellung mit der W2k8-Server DVD!

Es können keine Sicherungen auf Bandlaufwerke gemacht werden.
Es können keine einzelnen Dateien gesichert werden.
Sicherungs-Operatoren können keine geplanten Sicherungen einrichten.
Das System kann vollständig interaktiv mit dem Tool **wbadmin.exe** gesichert werden.

- Sie können den **gesamten Server samt Betriebssystem** sichern
- Ausschliesslich **Systemstatusdaten** und den **Verzeichnisspeicher ntds.dit** sichern
- Nicht autorisierende Daten wiederherstellen
- Autorisierende Daten wiederherstellen
- Mit **IFM** und einer Kopie von **ntds.dit** arbeiten (ntdsutil.exe)

Sicherungsmedien sind:
- Netzlaufwerke
- Wechselplatte die als Basisvolume konfiguriert sind
- DVDs
- CDs

Auf einem DC befinden sich folgende **Volumes**:
- Systemvolume
- Startvolume
- SYSVOL
- Das Volume mit der AD DS-Datenbank

- Das Volume mit den AD DS-Protokollen

Systemstatusdaten ohne weitere Rollen enthalten:
- Registrierung
- COM+-Klassenregistrierungsdatenbank
- Startdateien
- Dem Windows-Ressourcenschutz unterliegende Systemdateien
- AD DS-Verzeichnisdatenbank
- SYSVOL-Verzeichnis

Systemstatusdaten mit weitere Rollen enthalten zusätzlich:
- Die AD CS-Datenbank (Zertifikatdienst)
- Clusterdienstinformationen (Failovercluster)
- IIS-Konfigurationsdateien

wbadmin.exe (Windows Server Sicherung)

Windows Server Sicherung muss als **Feature** installiert werden.
Erfordert ein lokales Laufwerk für die Sicherung.

```
wbadmin start systemstatebackup
```

Wiederherstellung mit WinRE

WinRE kann entweder lokal installiert werden oder ist auf den W2k8-Server Installationsmedien zu finden.
Installieren Sie WinRE auf allen eingerichteten DCs. Dazu benötigen Sie zugriff auf das **Windows Automated Installation Kit** (WAIK)

Autorisierende und nicht autorisierende Wiederherstellung

Verwaltung der Systemleistung

- Task-Manager
- Ereignisanzeige
- Zuverlässigkeitsüberwachung
- Systemmonitor
- Windows-Systemressourcen-Manager (WSRM)

Task-Manager

taskmgrk.exe
Registerkarte: **Systemleistung/Leistung**

Dieses Tool stellt Statusinformationen in Echtzeit bereit.

- Ausgeführte Anwendungen
- Ausgeführte Prozesse
- Ausgeführte Dienste
- Leistung, einschliesslich CPU- und Arbeitsspeicherauslastung
- Netzwerknutzung, einschliesslich Nutzung der Netzwerkkarte (NIC)
- Derzeit angemeldete Benutzer

Swapping/Paging

Ständiges Auslagern ist ein typisches Problem auf Servern mit unzureichendem physischen Speicher, das oft durch langsame Systemreaktionen auffällt.

Ereignisanzeige

Eine **kostenfreie Datenbank** mit Windows-Ereignis-IDs finden Sie unter http://kb.prism-microsys.com/index.asp

Im Ordner: ***Windows-Protokolle*** befinden sich die Ereignisse für: **Anwendungen, Sicherheit, Einrichtung, System** und **weitergeleitete Ereignisse**.
Im Ordner: ***Anwendungs- und Dienstprotokolle*** sind die Ereignisse zu **AD-DS**.

- DFS-Replikation
- Verzeichnisdienst
- DNS-Server

Windows-Zuverlässigkeitsüberwachung

Ist darauf ausgelegt, die an einem System vorgenommenen Änderungen zu verfolgen. Jede Änderung am System wird in der Zuverlässigkeitsüberwachung protokolliert.

- Systemänderungen
- Softwareinstallationen / -deinstallationen
- Hardwarefehler
- Windows-Fehler

Windows-Leistungsüberwachung

Leistungsprotokolle und Warnungen, Leistungsratgeber für Server und Systemmonitor.

Windows-Systemressourcen-Manager (WSRM)

Muss als Feature hinzugefügt werden.

Im wesentlichen stellt der WSRM sicher, dass Anwendungen mit hoher Prioriät immer genügend Ressourcen zur Verfügung haben.

Wenn Anwendungen die Ressourcenzuweisungen überschreiten, kann der **WSRM** die Ausführung der Anwendung sogar stoppen und sicherstellen, dass andere Anwendungen auf demselben Server weiterhin ausgeführt werden können. Mit dem **WSRM** können Sie umfassend steuern, wie Anwendungen ausgeführt werden können und sollen.

Der WSRM unterstützt auch Warnhinweise und die Ereignisüberwachung.

- Verwenden vordefinierter oder benutzerdefinierter Richtlinien
- Nutzen von Kalenderregeln
- Automatisieren des Auswahlprozesses für Ressourcenrichtlinien

Active Directory Lightweight Directory Services (AD LDS)

Von den **fünf Active Directory-Technologien** unter W2k8-Server stellen die **Active Directory-Lightweight Directory Services** (AD LDS) die Technologie dar, die den **AD DS**-Domänendiensten am meisten ähnelt.

Die **AD LDS**, zuvor **Active Directory Application Mode** (ADAM) genannt, sind eine Technologie zur Unterstützung **verzeichnisfähiger Anwendungen** auf Anwendungsbasis und ohne erforderliche Änderungen des **Datenbankschemas** des Verzeichnisses des Netzwerkbetriebssystems, das unter den **AD DS** ausgeführt wird. Die **AD LDS** eignen sich besonders für Administratoren, die mit verzeichnisfähigen Anwendungen arbeiten möchten, ohne diese in das Verzeichnis ihres Netzwerkbetriebssystems zu integrieren.
Die **AD DS** unterstützen ebenfalls **verzeichnisfähige Anwendungen**. Ein sehr gutes Beispiel ist **MS Exchange Server 2007**. Alle Benutzerinformationen in Exchange Server werden vom Verzeichnis bereitgestellt. Da **Exchange** einen **GC** erfordert ist **AD DS** hier die bessere Lösung.

Die **AD LDS** kommt dann zum Einsatz wenn in einer Anwendung **schnelle Informationssuchen** erforderlich sind. Die Instanzen von **AD LDS** können an verschiedenen Orten im Netzwerk verteilt werden. Und replizieren sic h über die **Multimasterreplikation**. Zusammengefasst stellen die **AD LDS** eine abgespeckte, portierbare Version des von den **AD DS** gebotenen Verzeichnisdienstes dar. Zu den typischen Anwendungsbereichen zählen **Telefon-** und **Adressbücher**, **sicherheitsorientierte Anwendungen** sowie **Netzwerkkonfigurations**- und **Richtlinienspeicheranwendungen**.

Schemaänderungen dürfen nicht auf die leichte Schulter genommen werden, da ein **Objekt** oder **Attribut**, das Sie einmal dem **AD DS-Schema** hinzugefügt haben, nicht mehr entfernt werden kann!
Die **Replikationszeiten** können so erheblich verlängert werden.
Vermeiden Sie möglichst die Installation von AD LDS auf DCs.

Die **AD LDS** können auf **Mitglieds-** oder **eigenständigen Servern** ausgeführt werden, und für die Verwaltung sind nur **lokale Administratorrechte** erforderlich.
Die **AD LDS** ist lediglich eine Anwendung, die Installation ist deshalb einfach.

- Verwenden Sie die **AD LDS**, um mit Benutzerkonten in den AD DS verknüpfte Daten bereitzustellen.
- Sie können eine **AD LDS** Instanz zu Bereitstellen von **Authentifizierungsdiensten für Webanwendungen** wie **Microsoft SharePoint Portal Server** (MOSS)in einem Umkreisnetzwerk oder Extranet einsetzen.
- Sie können **mehrere Identitätsspeicher** zu einem **einzelnen Verzeichnisspeicher zusammenfassen**, Mithilfe eines Metaverzeichnisdienstes wie **MS Identity Integration Server** (MIIS), **MS Identity Lifecycle Manager** (MILM) oder dem kostenlosen **Identity Integration Feature Pack** (IIFP).
- Stellen Sie mit **AD LDS** abteilungsspezifische Anwendungen bereit.
- Sie können **ältere Verzeichnisanwendungen** in die AD LDS **migrieren**.

Wichtige Ports beim AD LDS:
Port 389 (Niemals für eine Instanz von AD LDS verwenden in einer Domäne!)
Port 636
Port >= 50000

Active Directory-Zertifikatdienste (AD CS) und PKI

Active Directory Certificate Services (AD CS)

Snap-In: ***Active Directory-Zertifikatdienste***
Tool: **certutil.exe**

AD CS eignet sich hervorragend für die Ausführung unter **W2k8-Hyper-V**.
Nach Installation des **AD CS-Dienstes** können Sie den Namen eines Servers nicht mehr ändern.
AD CS sollte nicht auf einem **DC** installiert werden.
AD CS kann nicht auf einem **Server Core** installiert werden. Ausserdem kann **AD CS** nicht auf Systemen mit **Itanium-Prozessoren** installiert werden.

Public Key Infrastructure (PKI) werden in modernen Unternehmen zunehmend zu Hauptelementen der Infrastruktur. In nahezu jedem Unternehmen werden gegenwärtig Zertifikate mit einem öffentlichen Schlüssel eingesetzt. Ob zum Absichern der **drahtlosen Kommunikation** zum Anbieten **sicherer kommerzieller Dienste auf Websites**, zum **integrieren von SSL** (Secure Socket Layer) mit **virtuellen privaten Netzwerken** oder bloss zum **Signieren von E-Mails** oder zur eigenen **Identifizierung in Webumgebungen**, überall arbeiten Unternehmen mit **PKI-Zertifikaten**. Das verwalten der PKI erfolgt unter W2k8 mithilfe der **Active Directory-Zertifikationsdienste** (AD CS).

PKI zeichnen sich dadurch aus, dass sie nicht allein auf Software basieren. Da **PKI-Zertifikate** die Aufgabe haben, anderen nachzuweisen, dass Sie derjenige sind, der Sie vorgeben zu sein, müssen administrative Prozesse eingerichtet werden, über die effektiv nachgewiesen werden kann, dass jede Person, die von Ihnen ein Zertifikat empfängt, tatsächlich auch die jeweilige Person ist. PKI garantiert dies.
Die **AD CS** haben die Aufgabe im internen wie externem Netzwerk die Authentifizierung und Autorisierung zu kontrollieren. Wenn Sie mithilfe von **AD CS** den Einflussbereich Ihres Unternehmens über die Grenze Ihres Netzwerks ausdehnen, müssen Sie mit einer Zertifizierungsstelle eines **kommerziellen Anbieters** zusammenarbeiten.

Wenn Sie sich beispielsweise über **HTTPS** mit einer Website verbinden, die ein **SSL-Zertifikat** enthält, dient dieses Zertifikat als Nachweis, dass Sie sich tatsächlich auf der gewünschten Website befinden. Wenn Sie das Zertifikat prüfen, erkennen Sie, dass es den **Servernamen**, den **Unternehmensnamen** und die **ausstellende Zertifizierungsstelle** enthält.

Die **Liste vertrauenswürdiger Zertifizierungsstellen** wird über die Updatemechanismen des ausgewählten Betriebssystems automatisch aktualisiert. Unter **WVista** und **W2k8-Server** wird diese Aktualisierung von einer **Gruppenrichtlinie** gesteuert.

Wenn Sie eigene Zertifikate ausstellen, d.h. Zertifikate, die nicht von externen Zertifizierungsstellen stammen, müssen Sie Ihr Unternehmen als vertrauenswürdige Zertifizierungsstelle den Computern der Benutzer hinzufügen, die diese Zertifikate verwenden sollen. Diese Vorgehensweise bietet sich an, wenn Sie mit Benutzern in Ihrem Unternehmen zusammenarbeiten, da Sie die Kontrolle über deren Computer haben. Sie wird jedoch problematisch bei Benutzern, deren Computer nicht unter Ihrer Obhut stehen.

Das Vertrauen einer PKI wird verkettet:
- Stammzertifikat
- Zwischenzertifikat
- Benutzerdefiniertes Zertifikat

Der Betrieb mehrere Technologien hängt von **PKI-Zertifikaten** ab. Gute Beispiel sind:
- **MS Exchange Server 2007**
- **MS Outlook Web Access** (OWA)

AD CS bietet mehrere Dienste:

- **EFS** basiert, Datendateien verschlüsseln
- **VPN**-Verbindungen verschlüsseln
- **E-Mail** Nachrichten absichern (**S/MIME**)
- Anmeldungen mit **Smartcards** absichern
- **Server** authentifizieren
- Die **drahtlose Kommunikation** absichern
- Daten gegen Manipulation schützen (**AD RMS**)

Die Komponenten von **AD CS** sind:

- Zertifizierungsstelle
  - Eigenständige Zertifizierungsstelle
  - Unternehmenszertifizierungsstelle
- Zertffifizierungsstellen für die Webregistrierung
- Online-Responder (Online Certificate Status Protocol, OCSP)
- Registrierungsdienst für Netzwerkgeräte (NDES/SCEP)

Eine **Zertifizierungsstellenhierarchie** basiert auf einer **Zertifikatverkettung**.

Es können **zwei**- oder **dreischichtige Zertifizierungsstellenhierarchien** gebildet werden.

Online-Responder dienen der Zusammenstellung von Systemen, um die hohe Verfügbarkeit dieses Dienstes sicherzustellen.
Um den Online-Responder zu konfigurieren sollten sie **Authority Information Access** (AIA) installieren.

Für die Installation des Registrierungsdienstes für Netzwerkgeräte benötigen Sie ein besonderes Benutzerkonto. Erstellen Sie ein Domänenkonto, und fügen Sie es der lokalen Gruppe **IIS_IUSRS** auf allen Servern hinzu, die diesen Dienst ausführen.

Unternehmenszertifizierungsstellen (CA)

Enterprise Root Certification Authority (CA)

Unternehmenszertifizierungsstellen können nur unter **W2k8-Server Enterprise Edition** und **W2k8-Server Datacenter Edition** ausgeführt werden.

Active Directory-Rechteverwaltungsdienst (AD RMS)

Die **Active Directory-Rechteverwaltungsdienste** (AD RMS) zuvor nur Rechteverwaltungsdienste genannt, dienen zur Ausdehnung des Einflussbereichs Ihres internen Netzwerks auf die Aussenwelt. Dieses Mal bezieht sich diese Ausdehnung auf **geistiges Eigentum**.
Die **AD RMS** arbeiten mit einem speziellen **AD RMS-Client**, um vertrauliche Informationen zu schützen. Der Schutz wird von der **Serverrolle AD RMS** bereitgestellt, die für die Verwaltung von Zertifikaten und Lizenzierung sorgt. Konfigurations- und Protokollinformationen werden dauerhaft in einer Datenbank gespeichert.

Der **MS Message Queing-Dienst** stellt die Koordination von Transaktionen in verteilten Umgebungen sicher.
Die **AD RMS** nutzt die **AD DS** zum Authentifizieren von Benutzern und überprüfen, ob diese zur Nutzung des Dienstes befugt sind.
Die **AD RMS** bieten nun eine direkte Integration mit den **Active Directory-Verbunddiensten** (AD FS), wodurch Die Ihre Rechteverwaltungsrichtlinien über die Firewall hinaus auf Ihre Partner ausdehnen können. Dies bedeutet, dass Ihre **Partner** keine eigenen **AD RMS-Infrastruktur** benötigen, da sie über die **AD FS** Ihre **AD RMS-Infrastruktur** für den Zugriff auf **AD RMS-Features** nutzen können.

Um Informationen mithilfe der **AD RMS** zu schützen, muss der **AD RMS-Server Rechtekontozertifikate** ausstellen.
AD RMS arbeitet mit **Lizenzen** im **XrML-Format** (Extensible Rights Markup Language).

Digtital Rights Managemenent (DRM).

Die Lösung zielt auf folgende Probleme:
Kopierschutz von Word-Dokumenten, Power-Point Präsentationen, E-Mails und anderen Inhalten.
Bei der **Erzeugung der Informationen** können die Benutzer festlegen, **wer Informationen lesen, schreiben, ändern, drucken, übertragen** oder auf **sonstige Weise bearbeiten darf.**
Nutzungsrechte werden direkt in die erstellten Dokumente eingebettet, sodass die Informationen geschützt bleiben, auch wenn sie Ihren Einflussbereich verlassen. **Nutzungsrechte** werden in eine beliebige Form von **Binärdaten** integriert, welche die Nutzung innerhalb und ausserhalb Ihres Netzwerks sowie **online** und **offline** unterstützt.
Um mit den **AD RMS** arbeiten zu können, benötigen **Benutzer** ein **E-Mail-fähiges Konto** in einer **AD DS-Domäne**.

Durch die Implementierung von DRM können **E-Mail-Inhalte** nicht mehr **verfälscht** werden. Der Schutz geht über die Unternehmensgrenzen hinaus.

Wichtig ist die Verfassung von klaren Dokumentenschutzrichtlinien für die Benutzer.

Bei der Erstinstallation eines AD RMS-Servers erstellen Sie standardmässig einen **AD RMS-Stammcluster**. Ein **Stammcluster** dient zur Verarbeitung von Zeritifizierungs- und Lizenzierungsanforderungen. In einer **AD DS-Gesamtstruktur** kann nur **ein Stammcluster vorhanden sein**. Sie könne auch reine **Lizenzierungscluster** bilden. Neue **AD RMS-Server** werden automatisch in den Cluster integriert.

- **Stammcluster** verarbeiten sämtliche **AD RMS-Vorgänge** und sind deshalb multifunktional.
- **Stamm-** und **reine Lizenzierungscluster** sind unabhängig, was bedeutet, dass sie nicht zum **Lastenausgleich** des Dienstes beitragen können. ***Wenn Sie alle Ihre Server als Stammserver installieren, sorgen sie automatisch für einen gegenseitigen Lastenausgleich.***

Die Phasen der Implementierung

- Die erste Phase konzentriert soch auf die interne Nutzung geistigen Eigentums.
- Die zweite Phase dreht sich um die gemeinsame Nutzung von Inhalten mit Partnern.
- In der dritten Phase Nutzung über die Unternehmensgrenzen hinweg.

Bereitstellungsszenarien

- Einzelserverbereitstellung
- Interne Bereitstellung
- Bereitstellung im Extranet
    - Extranetcluster-URL hinzufügen

Die Verwaltungsrollen der AD RMS:

- AD RMS-Organisationsadministratoren
- AD RMS-Vorlagenadministratoren
- AD RMS-Prüfer
- AD RMS-Dienst

Da alle diese **Gruppen** lokal sind, müssen Sie entsprechende **Gruppen** in Ihrem **AD DS-Verzeichnis** erstellen und ***diese Gruppen den lokalen Gruppen auf allen AD RMS-Servern hinzufügen***.

Dienstverbindungspunkt

Zum **Registrieren** des **AD RMS-Dienstverbindungspunkts** müssen Sie mit einem **Benutzerkonto mit Schreibzugriff** auf den Container **Dienste** in den **AD DS** angemeldet sein (**Organisations-Admins**).

Datenbank

Für den Betrieb der AD RMS sind drei Datenbanken erforderlich.

- Konfigurationsdatenbank
- Protokollierungsdatenbank
- Verzeichnisdienstedatenbank

Als Datenbank eignet sich ein dedizierter Server mit **MS SQL 2005** oder **MS SQL 2008**.

Active Directory-Verbunddienste (AD FS)

Active Directory Federation Services (AD FS)

AD FS wurde eingeführt bei **W2k3 R2**.

Allgemein gesehen handelt es sich bei den **AD FS** um ein Modul für die **einmalige Anmeldung** (Single Sign On, SSO), das Benutzern Ihrer externen, webbasierten Anwendungen den Zugriff und die Authentifizierung über einen Browser ermöglicht.
Das Hauptmerkmal der **AD FS** ist jedoch, dass für die Authentifizierung eines Clients der **interne Authentifizierungsspeicher der eigenen Domäne des Benutzers verwendet wird** und die **AD FS** nicht über einen **eigenen Speicher** verfügt. Darüber hinaus wird die **ursprüngliche Authentifizierung** des Clients genutzt, die dieser in seinem eigenen Netzwerk durchgeführt hat, und diese Authentifizierung wird an alle Internetanwendungen übergeben, die **AD FS-fähig** sind.
Die Vorteile liegen auf der Hand. Organisationen müssen lediglich einen einzigen **Authentifizierungsspeicher** für ihre eigenen Benutzer verwalten, die Verwaltung **sekundärer Speicher** ist nicht erforderlich.
Mithilfe der **AD FS** ist es möglich, mit wenig Aufwand **B2B-Partnerschaften** (Business-to-Business) aufzubauen. Dabei gibt es zwei Kategorien:

- Ressourcenorganisationen
- Kontoorganisationen

Die **AD FS** kennt vier Rollendienste:

- Verbunddienst
- Verbunddienstproxy
- Ansprüche unterstützender Agent
- Windows-Token-basierter Agent

Die **AD FS-Entwürfe**:

- Federated-Web-SSO
    - Dieses Modell umfasst in der Regel sieben Firewalls
- Federated-Web-SSO mit Gesamtstrukturvertrauensstellung
- Web-SSO

Grundlegende **AD FS-Komponenten**:

- Ansprüche
- Cookies

    - Authentifizierungscookies
    - Kontopartnercookies
    - Abmeldecookies
- Zertifikate
    - Verbundserver
    - Verbunddienstproxies
    - AD FS-Web-Agent

Die Hauptaufgabe eines **Umkreisnetzwerks** besteht darin, die im Netzwerk enthaltene Firewall so sicher wie möglich zu machen. Dies hat jedoch Auswirkungen auf die Partnerschaften.

Domänen innerhalb der gleichen Gesamtstruktur verwenden automatisch **transitive Vertrauensstellungen**, und Domänen aus unterschiedlichen Gesamtstrukturen nutzen zur Freigabe von Sicherheitskontexten explizite Vertrauensstellungen. Über eine Gesamtstrukturvertrauensstellung könnten Partner die erweiterten Sicherheitskontexte ihrer eigenen internen Gesamtstruktur auf andere, vertraute Partnergesamtstrukturen erweitern. Die Implementierung von Gesamtstrukturvertrauensstellungen hat jedoch zwei bedeutende Auswirkungen:

- Zur Unterstützung von **AD DS-Datenverkehr** ist die Öffnung von bestimmten Ports in der Firewall erforderlich.
- Zum anderen kann die Verwaltung mehrerer Vertrauensstellungen äusserst arbeitsintensiv werden, wenn die Partnerschaften zu gross werden.

Der **AD DS-Datenverkehr** wird beispielsweise mithilfe von **LDAP** auf Port **389** oder vorzugsweise über das sichere **LDAP/S** auf Port **636** geleitet. Wenn darüber hinaus der **GC-Datenverkehr** weitergeleitet werden muss, müssen Sie Port **3268** oder vorzugsweise Port 3269 öffnen.

Die ideale Firewall verwendet nur einen Satz an Schlüsselports:

- Port 53 DNS-Datenverkehr
- Port 80 HTTP-Daten
- Port 443 HTTPS-Daten
- Port 25 SMTP-Datenverkehr

Alle weiteren Ports sollten eigentlich geschlossen sein.

Die AD FS wurde für die Bereitstellung von Funktionen für die Gesamtstrukturvertrauensstellung oder die explizite Vertrauensstellung entwickelt. Jedoch nicht über die LDAP-Ports, sondern über die gemeinsamen HTTP-Ports 443.

Um Ihre interne Autorität zu erweitern, stellen die **AD FS** Erweiterungen für interne Gesamtstrukturen bereit und ermöglichen Organisationen den Aufbau von Partnerschaften, ohne dafür zusätzliche Ports in den Firewalls öffnen zu müssen.

Wichtiges Event für die Kontrolle der Funktionalität: **674**

Upgrades

Während des **Upgrades der AD FS** werden alle Dienste standardmässig auf die Verwendung des Kontos ***Netzwerkdienst*** zurückgesetzt.

Terminaldienste

In **W2k8-Server** wird **Remotedesktop** gewöhnlich für die **Remoteverwaltung** verwendet und die **Terminaldienste** werden für die Ausführung von **Anwendungen** eingesetzt.

Die **Terminaldienste** ermöglichen es Remotebenutzern, auf einem W2k8-Server ***interaktive Desktopsitzungen und Anwendungssitzungen*** durchzuführen.
Remotedesktop und die **Terminaldienste** sind eng miteinander verwandt. Erstens verwenden beide Technologien dieselbe Clientsoftware namens **Remotedesktopverbindung** (mstsc.exe) . Zweitens sind auch die Serverkomponenten beider Features im Wesentlichen gleich. Terminaldienst und Remotedesktop sind auf denselben Dienst angewiesen, nämlich auf den Dienst Terminaldienst. Und schliesslich richten Remotedesktop und die Terminaldienste ihre Sitzungen beide mit demselben Protokoll **Remote Desktop Protocol** (RDP) und demselben **TCP-Port 3389** ein.
Bei **Remotedesktop** können ***nur zwei Benutzer gleichzeitig*** mit einer aktiven Desktopsitzung verbunden sein. Bei einem Server auf dem die **Terminaldienste** installiert sind gilt diese Einschränkung nicht.

Leistungsmerkmale der Terminaldienste:

- Mehrbenutzerfähigkeit
- RemoteApp
- Terminaldienste-Webzugriff
- Terminaldienste-Sitzungsbroker
- Terminaldienstegateway

Remotedesktop

Der wichtigste Vorteil von Remotedesktop gegenüber den Terminaldiensten besteht darin, dass die Funktion bereits in W2k8-Server integriert ist und nicht den Kauf von Terminadienste-Clientzugriffslizenzen erfordert. Die Aktivierung von Remotedesktop erfolgt über eine einzige Option im Dialogfeld Systemeigenschaften (**control sysdm.cpl**). In der **Windows-Firewall** wird automatisch eine Remotedesktop-Ausnahme eingerichtet.
Die Authentifizierung auf Netzwerkebene (Network Level Authentication, NLA) ist eine Funktion des Remotedesktopprotokolls 6.0, die dafür sorgt, dass vor dem vollständigen Aufbau einer Remotedesktopverbindung zwischen zwei Computern eine Authentifizierung des Benutzers stattfindet.

Configuration: Remotedesktopverbindung

Benutzerkonten

Das Attribut **sAMAccountName** eines Benutzers (der Prä-Windows 2000-Anmeldename) muss innerhalb der gesamten Domäne eindeutig sein.
Je nach Grösse des Unternehmens kann es bei Verwendung des Namens und Vornamens zu Duplikaten kommen. Dieses Problem können Sie umgehen, indem Sie für den **sAMAccountName** die Personalnummer oder ein anderes eindeutiges Attribut des Benutzers verwenden.

userPrinzipalName (UPN) setzt sich aus dem Anmeldenamen und einem UPN-Suffix zusammen. Der UPN muss für die gesamte Domäne eindeutig sein. Daher sollten Sie die Verwendung von E-Mail-Adressen als UPN in Betracht ziehen.

RDN muss in der Domäne eindeutig sein.

CN könnte z.B. die Personalnummer umfassen, wie z.B. Scott Miller (645928).

displayName wird in der globalen Adressliste (Global Address List, GAL) Exchange angezeigt.

inetOrgPerson Objektklasse.

Mit **redirusr.exe** kann der Standardcontainer für neue Benutzer umgeleitet werden.

Gruppen

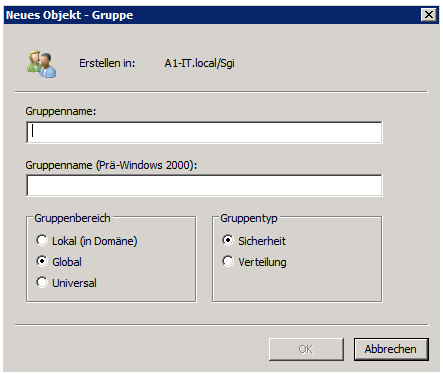


Abbildung 8: Gruppen

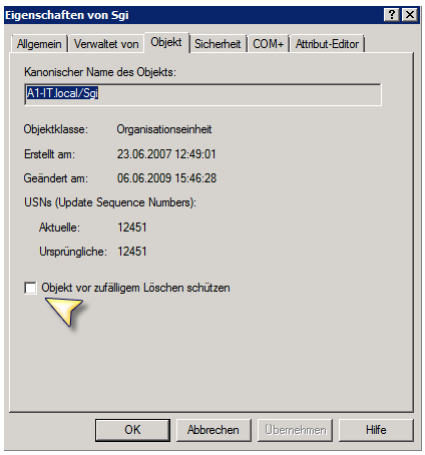


Abbildung 9: Objekte schützen

Achtung um das Objekt zu schützen muss die **Ansicht erweiterte Features** ausgewählt sein.

Verteilergruppen

Verteilergruppen werden vorwiegend von E-Mail-Anwendungen genutzt. Diese Gruppen sind nicht sicherheitsaktiviert, d.h. sie verfügen nicht über **SIDs**, und daher kann ihnen keine Berechtigung für Ressourcen erteilt werden. Durch das versenden einer Nachricht an eine Verteilergruppe erhalten alle Mitglieder der Gruppe die Nachricht.

Sicherheitsgruppen

Sicherheitsgruppen sind Sicherheitsprinzipale mit **SIDs**.

Gruppenbereich

Lokal

Lokale Gruppen tragen diesen Namen zu Recht, sie werden auf einem einzelnen Computer definiert und sind auch nur dort verfügbar.

Domänenlokale Gruppen

Domänenlokale Gruppen werden vorwiegend für die Verwaltung von Ressourcenberechtigungen verwendet.

Global

Globale Gruppen werden, badierend auf Geschäftsrollen, vorwiegend für die Definition von Domänenobjektsammlungen verwendet.

Universal

Universelle Gruppen sind in Gesamstrukturen mit mehreren Domänen nützlich.

Computer

Computer sind auch Personen –zumindest in Active Directory.

Bei Computern in einer Domäne handelt es sich, wie auch bei Benutzern, um Sicherheitsprinzipale. Sie verfügen über ein Konto mit einem Anmeldenamen und einem Kennwort, das von MS Windows automatisch z.B. alle 30 Tage geändert wird.

Wird ein Computer einer Domäne hinzugefügt, delegiert er die **Benutzerauthentifizierung** an die Domäne. Meldet sich ein Benutzer mit einem Domänenkonto an dem Computer an, so wird die **Benutzerauthentifizierung** nun über einen **Domänencontroller** und nicht mehr über die **SAM** vorgenommen.

Wenn der sichere Kanal nicht aufgebaut werden kann, muss er zurückgesetzt werden. Viele Administratoren entfernen hierfür den Computer aus der Domäne, platzieren ihn in einer Arbeitsgruppe und fügen ihn anschliessend wieder zur Domäne hinzu. Diese Vorgehensweise ist nicht empfehlenswert. Dabei geht die **Gruppenmitgliedschaft** und die **SID** verloren, auch wenn ein gleichnamiges Computerkonto eröffnet wird Die empfohlene Vorgehensweise ist, dass Computerkonto zurückzusetzen.

Es wird empfohlen die Standardeinstellungen für die Benutzer zum erstellen von Computerkonten einzuschränken. Attribut **ms-DS-MachlneAccountQuota = 0**.

Der lokale Identitätsspeicher auf jedem Computer wird als **SAM-Datenbank** (Security Accounts Manager, Sicherheitskontenverwaltung) bezeichnet.

LSA-Schlüssel (Local Security Authority, lokale Sicherheitsautorität)

Voraussetzungen Computer zu Domäne hinzufügen

1. Ein Computerobjekt muss im Verzeichnisdienst erstellt werden.
2. Sie müssen über die geeigneten Berechtigungen für das Computerobjekt verfügen. Die Berechtigungen ermöglichen es Ihnen, einen Computer mit dem gleichen Namen wie das Objekt zur Domäne hinzuzufügen.
3. Sie müssen ein Mitglied der kokalen Gruppe Administratoren auf dem Computer sein, um Änderungen an der Domänen- oder Arbeitsgruppenmitgliedschaft des Computers vorzunehmen.

Mit **redircmp.exe** kann der Standardcomputercontainer umgeleitet werden.

NETLOGON Fehler mit der Meldung "***der RPC-Server ist nicht verfügbar***" weisen auf einen Fehler beim sicheren Kanal hin. Abhilfe schafft hier ein zurücksetzen des Computerkontos.

Gruppenrichtlinien

Die Ziele ➔ Erhöhte Sicherheit, geringere Kosten, verbesserte Benutzerproduktivität.

Gruppenrichtlinien sind ein Windows-Feature, mit dem Sie Benutzer- und Computerkonfigurationen über einen zentralen Verwaltungspunkt verwalten und Änderungen daran vornehmen können.

In einer durch eine gut umgesetzte **Gruppenrichtlinieninfrastruktur** verwalteten Umgebung müssen nur sehr wenige oder gar keine Konfigurationen direkt an einem Desktopcomputer vorgenommen werden. Die gesamte Konfiguration wird über die Einstellungen in **Gruppenrichtlinienobjekten** (Group Policy Object, GPO) definiert.

Softwareinstallationen sind eine Aufgabe, die über Gruppenrichtlinien automatisiert und verwaltet werden können. Die Gruppenrichtlinien für die **Softwareinstallation** (Group Policy Software Installation, GPSI) wird von der *clientseitigen Erweiterung* für die Softwareinstallation unterstützt. Sie können ein **GPO** für die Installation von einem oder mehreren Softwarepaketen konfigurieren.
Der **Gruppenrichtlinienclient** kann eine langsame Verbindung (< 500 KBit/s) erkennen und die Installation starten oder verhindern.

Beim Installieren der **AD-DS** werden **zwei Standard-GPOs** erstellt:

- Default Domain Policy
- Default Domain Controllers Policy

Richtlinieneinstellungen

Die kleinste Komponente einer Gruppenrichtlinie ist eine einzelne **Richtlinieneinstellung**, oftmals auch einfach als **Richtlinie** bezeichnet.
Richtlinieneinstellungen werden in einem **Gruppenrichtlinienobjekt** (Group Policy Object, GPO) definiert und gespeichert.

- Regedit Ausführung verhindern
- Lokales Administratorenkonto deaktivieren
- Softwareinstallation ➔ GPSI

Gruppenrichtlinienobjekte

Bei einem GPO handelt es sich um eine **Sammlung an Konfigurationseinstellungen**, die von den **CSEs** der Computer verarbeitet werden. Bis der Bereich für ein **GPO** festgelegt ist, wird es nicht auf Benutzer oder Computer angewendet.

Gruppenrichtlinienobjekte werden über die **Gruppenrichtlinienverwaltung** (Group Policy Management Console, GPMC) verwaltet.

In einer neuen **GPO** sind alle **Richtlinieneinstellungen** als *nicht konfiguriert* eingestellt.

Zum Verwalten des **Bereichs** von **GPOs** stehen verschiedene Methoden zur Auswahl. Die erste wird als *Verknüpfung des Gruppenrichtlinenobjektes* bezeichnet.
GPOs können in **Active-Directory** mit **Standorten**, **Domänen** und **OUs** verknüpft werden.
Der GPO-Bereich kann darüber hinaus über einen der beiden folgenden Filtertypen eingeschränkt werden: Sicherheitsfilter, die globale Sicherheitsgruppen festlegen, auf die das GPO angewendet werden soll oder nicht, und WMI-Filter (Windows Management Instrumentation), die anhand der Merkmale eines Systems wie z.B. einer Betriebssystemversion oder der Menge an freiem Festplattenplatz einen Bereich festlegen.
Verwenden Sie **Sicherheits-** und **WMI-Filter** , um den **Bereich** im **ursprünglichen Bereich** einzuschränken oder festzulegen, der durch die GPO-Verknüpfung erstellt wurde.

Lokale Gruppenrichtlinienobjekte sind vorhanden auch wenn der Computer Teil einer Domäne, Arbeitsgruppe oder einer Umgebung ohne Netzwerk ist! Es wird im folgenden Verzeichnis gespeichert:
`%SystemRoot%\System32\GroupPolicy`

WVista und **W2k8-Server** Systeme verfügen über mehrere lokale Gruppenrichtlinienobjekte.

Gruppenrichtlinienvorlagen sollten als **.adml** und **.admlx** Dateien (Sprachspezifische Dateien) gespeichert werden. Ein gemischter Betrieb auch mit **.adm-Dateien** funktioniert.
Speicherort: **Fehler! Linkreferenz ungültig.**
Speicherort bei lokaler oder Remoter-Anmeldung:
`%SystemRoot%\SYSVOL\Domain\policies\PolicyDefinitions`

Bei den Dateien handelt es sich um Text-Dateien.

ADMX Files

Die neuen **WVista**- und **W2k8-Server GPOs** können nur auf **WVista** oder **W2k8-Server Maschinen** mit **gpmc.exe** administriert werden.

Vererbung und Rangfolge

Die Anwendung der **GPO** wird über die **Rangfolge** geregelt. Eine **GPO** mit einer höheren Rangfolge hat Vorrang vor einer GPO mit niedrigerer Rangfolge. Je kleiner der Zahlenwert, d.h. je näher er am Wert 1 liegt, umso höher ist die Priorität. Eine **GPO** mit einem Wert 1 hat demnach vor allen anderen GPOs Vorrang.
Standardmässig ist das Verhalten von Gruppenrichtlinien festgelegt, dass mit einem in der Struktur höher gelegenen Container verknüpfte **GPOs** von dem darunter gelegenen Containern übernommen werden.

Die **Standardreihenfolge** für die Vererbung ist: **Standort, Domäne, OU**

Vererbung deaktivieren
Diese Option sollte wenn überhaupt, nur äusserst selten verwendet werden.

Verknüpfung erzwingen
Eine erzwungene Vererbung wird auf alle untergeordneten Container angewendet, selbst wenn für diese Container die Option ***Vererbung deaktivieren*** verwendet wurde.
Ausserdem werden durch die Auswahl dieser Option alle in Konflikt stehenden Richtlinien überschrieben.

Sicherheitsfilter

Damit können Gruppen definiert werden für welche die GPO angewendet werden soll.
Authentifizierte Benutzer
Administratoren etc.

WMI-Filter

WMI verwendet die Abfragesprache: **WMI Query Language, WQL**
Über WMI-Abfragen können Systeme basierend auf Merkmalen gefiltert werden, z.B. Prozessorgeschwindigkeit, Festplattenkapazität, IP-Adresse, Betriebssystemversion und Service-Pack Level.
Ein **GPO** kann mit nur einem **WMI-Filter** gefiltert werden. Aber ein WMI-Filter kann auf mehrere **GPOs** angewendet werden.

Achtung! WMI-Filter werden von Computern mit **W2k** nicht verarbeitet und der Rückgabewert der Filterung ist immer True.

```
Select * FROM Win32_OperatingSystem WHERE Caption""Microsoft Windows XP Professional" AND
CSDVersion= "Service Pack 3"
```

Loopbackrichtlinienverarbeitung

Durch die Loopbackrichtlinienverarbeitung **ändert das System die Art der Anwendung von GPOs während der Benutzerrichtlinienverarbeitung**. Im Modus Ersetzen werden Benutzerkonfigurationseinstellungen von GPOs nicht angewendet, in deren Bereich sich der angemeldete Benutzer befindet. Stattdessen werden nur Benutzerkonfigurationseinstellungen von GPOs angewendet, in deren Bereich sich der Computer befindet.

Kann angewendet werden um Computer in Konferenzräumen oder Laptop's zu steuern.

Richtlinienergebnissatz (RSoP)

Der **Richtlinienergebnissatz** (Result Set of Policy, RSoP) stellt die tatsächlichen Auswirkungen von GPOs dar, die auf einen Benutzer oder Computer angewendet werden, Hierbei werden GPO-Verknüpfungen, Ausnahmen wie erzwungene und deaktivierte Vererbung sowie die Anwendung von Sicherheits- und WMI-Filter berücksichtigt.
Der **RsOP** kann Abfragen für lokale und Remotecomputer durchführen.
Die Durchführung einer **RsOP-Analyse** ist ein Beispiel für **Remoteverwaltung**.
Zur Analyse kann auch der **Gruppenrichtlinienergebnis-Assistent**, oder **gpresult.exe** eingesetzt werden.
Sie müssen in der Lage sein, den **Richtlinienergebnissatz** (Result Set of Policy, RSoP) zu verstehen und zu bewerten.

Gruppenrichtlinienergebnis-Assistent

Voraussetzungen:

1. Sie müssen für den Zielcomputer über Anmelderechte als Administrator verfügen.
2. Auf dem Zielcomputer muss WXP oder höher ausgeführt werden.
3. Sie müssen über WMI-Zugriff auf dem Zielcomputer verfügen (Port: 135/445)
4. Der WMI-Dienst muss auf dem Zielcomputer gestartet sein.
5. Der Benutzer muss sich mindestens einmal an dem Computer angemeldet haben.

Gruppenrichtlinienaktualisierung

Die Anwendung von Richtlinien wird als Gruppenrichtlinienaktualisierung bezeichnet.

Richtlinieneinstellungen im Knoten ***Computerkonfiguration*** werden beim Startvorgang des Systems und danach alle **90-120 Minuten** angewendet.

Richtlinieneinstellungen im Knoten ***Benutzerkonfiguration*** werden bei der Anmeldung und danach alle **90-120 Minuten** angewendet.

```
gpupdate /force
gpupdate /target:<Computer>
gpupdate /target:<User>
gpupdate /logoff
gpupdate /boot
```

Client-Side Extensions (CSEs) sind Dienste welche auch als Gruppenrichtlinienclients bezeichnet werden. Sie werden beim Systemstart automatisch gestartet.
Systemstart:

1. Der Systemdienst **Remoteprozeduraufrufe** (Remote Procedure Call System Service, RPCSS) wird gestartet.
2. **MUP** (Multiple Universal Naming Convention Provider) wird gestartet.

Wenn Benutzer in Ihrer Umgebung auf ihren Computern als **Administratoren** angemeldet sind, sollten Sie **CSEs** unter Umständen so konfigurieren, dass Richtlinieneinstellungen auch dann erneut angewendet werden, wenn am Gruppenrichtlinienobjekt keine Änderung vorgenommen wurden. Auf diese Weise wird die durch einen Administratorbenutzer geänderte Konfiguration, die nicht mehr mit der Richtlinie übereinstimmt, bei der nächsten Gruppenrichtlinienaktualisierung zurückgesetzt, sodass die Übereinstimmung mit der Richtlinie wiederhergestellt wird. Konfigurieren Sie hierzu eine GPO für Computer und definieren Sie die Einstellungen in folgendem Verzeichnis:

```
Computerkonfiguration\Richtlinien\Administrativer Vorlagen\System\Gruppenrichtlinie
➔ Registrierungsrichtlinienverarbeitung aktivieren auch ohne Änderungen
```

Sie sollten die Richtlinieneinstellung ***Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten*** in jedem Fall für alle WXP und WVista-Clients aktivieren. Ohne diese Einstellung wird standardmässig nur eine **Hintergrundaktualisierung** durchgeführt.

```
Computerkonfiguration\Richtlinien\Administrativer Vorlagen\System\Anmelden
```

GPO-Replikation

Verzeichnisreplikations-Agent (Directory Replication Agent, DRA). Die Technik basiert auf der Konsistenzprüfung mittels **Knowledge Consistency Checker** (KCC)
Für die Gruppenrichtlinienvorlagen im Verzeichnis **SYSVOL** wird über eine der beiden Technologien eine Replikation durchgeführt. Der Dateireplikationsdienst (File Replication Service, FRS) wird zum replizieren des Verzeichnisses **SYSVOL** in Domänen verwendet, in denen **W2k8-Server**, **W2k3-Server** und **W2k-Server** ausgeführt wird. Wenn alle Domänencontroller **W2k8-Server** ausführen, können Sie für die Replikation **DFS-R** (Distributed File System Replication) festlegen.

GPOs für den Helpdesk

Die vom Supportpersonal verwendeten Anmeldekonten **müssen Mitglied der lokalen Administratorengruppen auf dem Clientcomputer sein**. Es ist jedoch nicht erforderlich, dass das Supportpersonal der **Gruppe Domänen-Admins** angehört. **Eine Platzierung in dieser Gruppe wird nicht empfohlen**. Stattdessen sollten die Clientsysteme so konfiguriert werden, dass der Gruppe der lokalen Administratoren eine Benutzergruppe hinzugefügt wird, welche die Supportmitarbeiter repräsentiert. **Richtlinien für eingeschränkte Gruppen** ermöglichen genau diese Konfiguration.

Bei der Definition dieser **GPO** ist den Optionen **Mitglied von** und **Mitglieder dieser Gruppe** Beachtung geschenkt werden. Sowie der Rangfolge der **GPOs**.

Einstellungen vom Typ: ***Mitglied von*** **sind kumulativ**
Einstellungen vom Typ: ***Mitglieder der Gruppe*** **sind endgültig, autorisierend**

Softwareinstallation (GPSI)

Die Gruppenrichtlinie für die Softwareinstallation (Group Policy Software Installation, GPSI) wird zur Erstellung einer verwalteten Softwareumgebung verwendet. Die Gruppenrichtlinie für die Softwareinstallation verwendet den Windows Installerdienst zum installieren, warten und entfernen von Softwarekomponenten. Das Windows Installer-Paket ist eine Datei mit der Erweiterung **.msi**.

Windows Installer-Pakete können mithilfe der folgenden Dateitypen angepasst werden:

- Transformationsdatei (.mst)

- Patchdatei (.msp)

Es ist nicht möglich **.mst** oder **.msp**-Dateien eigenständig bereitzustellen!

Der **Softwareverteilungspunkt** ist einfach ein freigegebener Ordner. Wichtig ist das Benutzer **Lese-** und **Ausführungsberechtigungen** besitzen.

GPO: ***Benutzerkonfiguration\Richtlinien\Softwareeinstellungen\Softwareinstallation***

Standardmässig verarbeitet die **GPSI** keine Gruppenrichtlinieneinstellungen über **langsame Verbindungen** (<500KBit/s).

zugewiesen
Die Installation der Anwendung erfolgt, wenn der Benutzer die Anwendung zum erstenmal im Startmenü auswählt oder ein verknüpftes Dokument öffnet.

veröffentlichen
Wenn Sie Anwendungen für Benutzer veröffentlichen, werden die Anwendungen auf den Computern der Benutzer nicht als installiert angezeigt. Stattdessen erscheint die Anwendung als verfügbare Anwendung, die vom Benutzer über die Option ***Software*** in der ***Systemsteuerung*** oder über die Option ***Programme und Features*** installiert werden können.

Sicherheitseinstellungen

Die Anzahl der Sicherheitseinstellungen die verwaltet werden können ist enorm und leider gibt es **keine Zauberformel**, welche die perfekte Sicherheitskonfiguration auf einem Server anwendet. Aus diesem Grund müssen Sie die erforderlichen Sicherheitseinstellungen für die Server in Ihrer Organisation **selbst ermitteln und konfigurieren** und Sie müssen darauf vorbereitet sein, diese Einstellungen in einer Weise zu verwalten, welche die **Sicherheitskonfiguration zentralisiert und optimiert**.

Sicherheitsvorlage

Ordner: **Documents\Security\Templates**

Eine **Sicherheitsvorlage** ist eine Sammlung aus Konfigurationseinstellungen, die als Textdatei mit der Erweiterung **.inf** gespeichert wird.
Wenn Sie einen **Server installieren** oder ihn zu einem **Domänencontroller heraufstufen**, wird von Windows eine **Standardsicherheitsvorlage** angewendet.

Einstellungstypen einer Sicherheitsvorlage:
- Kontorichtlinien
- Lokale Richtlinien
- Richtlinien für das Ereignisprotokoll
- Eingeschränkte Gruppen
- Systemdienste
- Registrierungsberechtigungen
- Dateisystemberechtigungen

Sie können **Sicherheitsvorlagen** auf verschiedene Arten bereitstellen, z.B. mithilfe von **Active Directory-Gruppenrichtlinienobjekten**, mit dem Snap-In ***Sicherheitskonfiguration und –analyse*** oder mit dem Dienstprogramm **secedit.exe**.

Um verschiedene Computer in nur einem Arbeitsschritt zu konfigurieren, können Sie eine Sicherheitsvorlage in das Gruppenrichtlinienobjekt (GPO) für eine **Domäne**, einen **Standort** oder eine **OU** in Active Directory importieren.

Zur Verwendung des Snap-In Sicherheitskonfiguration und –analyse müssen Sie zuerst eine **Datenbank** erstellen, die eine Sammlung der Sicherheitseinstellungen enthält. Die Datenbank ist die Schnittstelle zwischen den eigentlichen Sicherheitseinstellungen auf dem Computer und den Einstellungen, die in den Sicherheitsvolagen gespeichert sind. Erstellen Sie eine Datenbank inderm Sie mit der rechten Maustaste auf den Knoten ***Sicherheitskonfiguration und –analyse*** klicken.

Das Ändern eines Richtlinienwertes im Snap-In Sicherheitskonfiguration und –analyse ändert lediglich den Datenbankwert, nicht die eigentliche Computereinstellung. Die Änderung wird erst wirksam mit dem Befehl: **Computer jetzt konfigurieren**.

In einer Unternehmensumgebung sollte die **Sicherheitskonfigurationsdatenbank zentralisiert** werden, damit Administratoren bei der Ausführung des Sicherheitskonfigurations-Assistenten stets auf dieselbe Datenbank zurückgreifen.

scw.exe /kb <Datenbankspeicherort>

Secedit.exe

Secedit.exe ist ein Befehlszeilenprogramm, mit dem die gleichen Funktionen ausgeführt werden können wie mit dem Snap-In ***Sicherheitskonfiguration und –analyse***.
Der Vorteil von Secedit.exe besteht darin, dass Sie das Dienstprogramm über Skripts und Batchdateien aufrufen können.

Scwcmd.exe

Ordner: **%SystemRoot%\Security\Msscw\Kbs**

Überwachung

Komponenten: **Überwachungsrichtlinien**, **Überwachungseinstellungen** und **Sicherheitsprotokoll**

Wenn die **Überwachungsrichtlinie** deaktiviert ist, werden diese Aktivitäten nicht durch den Server überwacht.

Zur Objektüberwachung müssen der **SACL** Überwachungseinträge hinzugefügt werden.

- fehlgeschlagene Anmeldeversuche
- Zugriffsversuche auf die Active Directory-Objekte
  Es können Änderungen an den Werten nachvollzogen werden.
  Befehl: **auditpol.exe**
- Zugriffsversuche auf Unternehmensressourcen (Dateien, Ordner etc.)

Authentifizierung

Kennworteinstellungsobjekte (Password Settings Objects, PSO)
Das PSO mit dem Zahlenwert 1 hat die höchste Priorität.

Schreibgeschützte Domänencontroller (RODC)

>= W2k3 authentifiziert Benutzer über eines von zwei Protokollen:

- Kerberos v5
- NT LAN Manager (NTLM)

Mit **W2k8-Server** werden **fein abgestimmte Kennwortrichtlinien** eingeführt, mit denen unterschiedlich restriktive Kennwörter entsprechend den **Anforderungen von Gruppen oder Benutzern** in der Domäne angewendet werden können.

GPO:

```
Computerkonfiguration\Richtlinien\Windows-
Einstellungen\Sicherheitseinstellungen\Kontorichtlinien\Kennwortrichtlinien
```

Die Kennwörter werden als **Hashcodes** gespeichert.

Wenn Sie Kennwort- und Sperrichtlinien auf Benutzer in einer OU anwenden möchten, müssen Sie eine globale Sicherheitsgruppe erstellen, die alle Benutzer in der OU umfasst. Dieser Gruppentyp wird als **Schattengruppe** bezeichnet. Bei **Schattengruppen** handelt es sich um rein konzeptuelle und nicht um technische Objekte.

Vertrauensstellung

Eigentlich ist eine **Vertrauensstellung** eine logische Verknüpfung, die zwischen Domänen hergestellt wird, um die **Passthrough-Authentifizierung** zu ermöglichen.

Wenn Domäne A der Domäne B vertraut, dann ist Domäne A die **vertrauende Domäne**, und Domäne B ist die **vertraute Domäne**.

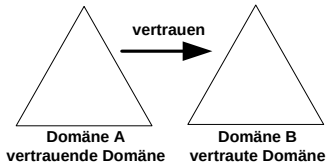


Abbildung 10: Vertrauensstellung

Eigenschaften:

- Transitiv
  - Ja/Nein
- Richtung
  - Uni- oder bidirektional
- Automatisch oder manuell
  - Automatisch erstellte Vertrauensstellungen sollten niemals gelöscht werden.

Vier Typen von Vertrauensstellungen müssen manuell erstellt werden:

- Shortcutvertrauensstellung
- Externe Vertrauensstellung
- Bereichsvertrauensstellung
- Gesamtstrukturvertrauensstellung

Read-Only Domain Controller (RODC)

Neu in W2k8-Server sind die **Schreibgeschützten Domänencontroller**. Sie bieten eine exzellente Lösung für **Remote Niederlassungen** und dabei optimale Sicherheit. Der RODC enthält eine **Kopie der Active Directory-Objekte** mit Ausnahme vertraulicher Informationen wie beispielsweise kennwortbezogene Eigenschaften.

Es kann eine **Kennwortreplikationsrichtlinie** (Passwort Replication Policy, PRP) für den **RODC** konfiguriert werden um die Benutzerkonten festzulegen, die der **RODC** zwischenspeichern darf. Hat sich der Benutzer über den **RODC** authentifiziert, speichert dieser die Anmeldeinformationen des Benutzers im Zwischenspeicher, sodass der **RODC** bei der nächsten Authentifizierung diese Aufgabe lokal ausführen kann.
Da der **RODC** nur einen Teilsatz der Benutzeranmeldeinformationen speichert, ist auch das Risiko begrenzt, falls ein solcher Domänencontroller **angegriffen** oder **gestohlen** wird. Es müssen nur die Kennwörter geändert werden welche sich im Zwischenspeicher des **RODCs** befanden.
Wenn Sie die **Anmeldeinformationen** von bestimmten Benutzern im Zwischenspeicher aller RODCs in der Domäne speichern möchten, fügen Sie diese Benutzer der Gruppe ***Zulässige RODC-Kennwortreplikationsgruppe*** hinzu.

Wenn sich in einer Zweigstelle kein Domänencontroller befindet, werden Authentifizierungs- und **Dienstticketaktivitäten** über die WAN-Anbindung an den Hub-Standort weitergeleitet.

Sie können sich ein **Dienstticket** als einen Schlüssel vorstellen, der von einem Domänencontroller an einen Benutzer ausgegeben wird. Mit diesem Schlüssel kann der Benutzer eine Verbindung mit einem Dienst wie beispielsweise den **Datei- und Druckerdienst** auf einem Dateiserver herstellen.

Voraussetzungen

- Die **Gesamtstrukturfunktionsebene** muss **W2k3** oder höher sein
  - Siehe Active Directory-Domänen und –Vertrauensstellungen
- Ein **W2k8-Server** mit Schreibberechtigung muss vorhanden sein.
- **adprep /rodcprep** (nur wenn nicht W2k8-Homogen)
  - Damit DNS-Anwendungsverzeichnispartitionen repliziert werden können.

Windows-Bereitstellungsinfrastruktur

Ein **Betriebssystem bereitzustellen** bedeutet, das Betriebssystem zu **installieren** und **einsatzbereit** zu machen. Die Methoden einschliesslich der Grundinstallation basieren auf der **Abbildtechnologie** mit **WIM-Dateien**.

Die **Basisabbilder** von **W2k8-Server** sind auf der **Windows-Produkt-DVD** in der Datei **install.wim** gespeichert.

Bereitstellungstechnologien:

- Windows PE
- ImageX
- Virtuelle Computer
- Windows-Bereitstellungsdienste
- Windows-Systemabbild-Manager
- Windows-Aktivierungsinfrastruktur
- MS System Center Configuration Manager 2007

Eine **WIM-Datei** (Windows Imaging Format) enthält eine oder mehrere Datenträgerabbilder im **WIM-Format**. Dabei handelt es sich um **Abbilder auf Dateibasis**. Das bedeutet, dass es sich um **Sammlungen von Volumendateien** handelt, also nicht einfach um Abbilder eines Datenträgers auf **Sektorbasis**. Der wichtigste Vorteil eines Abbilds auf Dateibasis gegenüber einem Abbild auf Sektorbasis besteht darin, ***dass man die Abbilder vor, während und nach der Bereitstellung ändern kann***.
Neben den **Nutzdaten** enthalten WIM-Dateien auch **Metadaten** auf **XML-Basis**.

- Sie können einen **Computer von einem Datenträgerabbild starten**, das in einer **WIM-Datei** enthalten ist, indem Sie das Abbild als startfähig kennzeichnen.
- **WIM-Dateien** unterstützen neben unkomprimierten Dateien (die schnellste Methode) auch zwei Komprimierungsarten, nämlich **Xpress** (schnell) und **LZX** (hochkomprimiert)
- Wenn Sie eine WIM-Dateiabbild aktualisiert haben, müssen Sie die dazugehörige **Katalogdatei** (.clg) neu erstellen.

Windows-Bereitstellungsmethoden

- Produkt-DVD
- Netzwerkfreigabe AIK und WIM-Dateien
- Windows-Bereitstellungsdienste
- System Center Configuration Manager 2007

Windows Automated Installation Kit (AIK)

Download: www.microsoft.com/downloads

Das **Windows AIK** bietet Administratoren und Computerherstellern Werkzeuge und die dazugehörige Dokumentation zur Durchführung von **unbeaufsichtigten Installationen** von **W2k8** und **WVista** und einigen älteren Versionen von MS Windows, einschliesslich **WXP** und **W2k3**.

Das **Windows AIK** enthält mehrere wichtige Bereitstellungstools:

- **Windows PE 2.0**
  - Im Prinzip können Sie Windows PE als Ersatz für startfähige MS-DOS-Disketten betrachten.
- **ImageX**
  - Die Hauptfunktion von ImageX ist die Erfassung eines Volumes in einem WIM-Dateiabbild und die Anwendung eines WIM-Dateiabbildes auf ein Volume.
- **Windows SIM**
  - Der Windows-Systemabbild-Manager ist ein Programm, mit dem sich **Antwortdateien** für die unbeaufsichtigte Installation von Windows erstellenlassen.
  - Windows SIM ersetzt den **Installations-Manager**

Sysprep

Das Programm **Sysprep** ist im Ordner **%SystemRoot%\System32\Sysprep** einer **WVista-** oder **W2k8-Server-Installation** zu finden. Die Aufgabe von Sysprep besteht darin, eine Masterinstallation des Betriebssystems **in eine allgemeine Form** zu bringen, die sich auf anderen Computern installieren lässt. **Sysprep** erstellt diese allgemeine Form eines Abbilds, indem es alle Einstellungen von der Masterinstallation entfernt, die nicht auf anderen Computern verwendet werden sollten, wie zum Beispiel den **Computernamen**, die **Domänenmitgliedschaft**, die **Zeitzone**, den **Produkt Key**, die **Sicherheitskennung (SID)** und verschiedene Benutzer- und Computereinstellungen. Eine mit Sysprep bearbeitete Installation bleibt auf der Festplatte und ist bereit, mit **ImageX** oder den **Windows-Bereitstellungsdiensten** erfasst, in eine WIM-Datei gespeichert und auf anderen Computern bereitgestellt zu werden.

Produkt-DVD

Der einfachste Weg, Windows auf neuer Hardware zu installieren, führt über die Windows-Produkt-DVD. Sie können eine Antwortdatei namens **Autounattend.xml** bereitstellen und damit den Vorgang so weit automatisieren, dass minimale interaktive Steuerung des Vorgangs erforderlich ist. Die Installation erfordert trotzdem vom **nichttechnischen Endanwender** umfangreiche Eingaben und Entscheidungen welche für eine Betriebssysteminstallation nicht zu empfehlen sind.

Netzwerkfreigabe AIK und WIM-Dateien

Für **20 oder weniger** neue Computer geeignet. Wenn keine **Active Directory-Domäne** noch das Netzwerkverwaltungsprogramm **System Center Configuration Manager 2007** zur Verfügung stehen. Die Voraussetzung hier ist eine ***schnelle und zuverlässige Datenübertragung***. Zur Installation sollten **Endanwender mit technischer Erfahrung** zur Verfügung stehen.

Es können **WIM-Dateiabbilder** oder ein **Setup-Programm** bereitgestellt werden.

Bei **WIM** wird der Computer mit Windows PE hochgefahren und die Installation mit dem Befehl: **[LW]:\setup /unattend:deploy_unattend.xml** gestartet.

Windows-Bereitstellungsdienste (WDS)

(Windows Deployment Services)

Die Windows-Bereitstellungsdienste (WDS) bestehen aus mehreren Komponenten und stellen die neuste Version der Remoteinstallationsdienste dar. Die Bereitstellungstechnologie basiert auf Server- und Abbildbasis.
Diese Bereitstellungstechnologie eignet sich auch für technisch unerfahrene Endanwender und lässt sich besser skalieren und verwalten als die anderen Technologien.
Der Zielcomputer findet mit einem **PXE-Startprozess** den Windows-Bereitstellungsdienstserver (WDS-Server).
Das **Startmenü** des WDS wird nur angezeigt, wenn es auf Ihrem WDS mehr als ein unterstütztes Startabbild gibt. Die maximale Anzahl angezeigter Startabbilder ist **13**.

Die **default.bcd** kann mit dem Programm **bcedit** bearbeitet werden.

Der **WDS-Server** fungiert als **PXE-Server** und **TFTP-Server**.

Achtung Standardmässig überwacht der WDS **Port 67**.

Rollen:

- Bereitstellungsserver

- Transportserver
    - **Multicast**-IP-Adressierung mit Trivial File Transfer Protocol (TFTP)
    - lässt sich nur mit **wdsutil** konfigurieren

Voraussetzungen:

- Active Directory
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- **NTFS-Volume** für die Speicherung der Installationsabbilder.
- Dauerhafte Hochgeschwindigkeitsverbindung zwischen den Windows-Bereitstellungsdiensteservern und den Zielcomputern.
- Damit ein **WDS-Clientcomputer** einen **WDS-Server** finden kann, muss er über eine **PXE-startfähige Netzwerkkarte** verfügen.

Der **WDS** eignet sich für die:

- Erstellung
- Anpassung
- Wartung
- Aktualisierung
- Installation

der Abbilder

Installieren des **WDS** mit **wdsutil**:

```
➔ wdsutil /Initialize-Server /reminst:Pfad\Ordnername
➔ wdsutil /Set-Server /AnswerClients:all
➔ wdsutil /Set-Server /UseDHCPPorts:no /DHCPoption60:yes
```

Standard-Speicherort für die Installationsabbilder: **%SystemDrive%\RemoteInstall**

Hinzufügen des **Startabbilds** mit **wdsutil**:

```
➔ wdsutil /Add-Image /ImageFile:DVD_LW:\sources\Boot.wim /IamgeType:boot
```

Hinzufügen des **Standardinstallationsabbilds** mit **wdsutil**:

```
➔ wdsutil /Add-Image /ImageFile:DVD_LW:\sources\Install.wim /IamgeType:install /ImageGroup:name
```

Die Einstellungen des **PXE-Servers**:

- Keinem Clientcomputer antworten
- Nur bekannten Clientcomputern antworten
- Allen(bekannten und unbekannten) Clientcomputern antworten

Ein **Startabbild** ist eine relativ kleine Windows-Abbilddatei (boot.wim), die Sie dazu verwenden können, einen frisch zusammengebauten Computer hochzufahren, auf dem noch kein Betriebssystem installiert ist. Im Gegensatz dazu handelt es sich bei einem **Installationsabbild** (install.wim) um das WVista- oder W2k8-Server Betriebssystem selbst.

Windows PE-CD erstellen

- Windows PE-Tools starten
- Eines der folgenden Commands wählen:
  (*Erstellt Verzeichnis ISO*)
    - ❑ copype.cmd x86 c:\WinPE_x86
    - ❑ copype.cmd amd64 c:\WinPE_amd64
    - ❑ copype.cmd ia64 c:\WinPE_ia64
- Eines der folgenden Commands wählen:
    - ❑ copy "c:\Program Files\Windows AIK\Tools\x86\imagex.exe" c:\WinPE_x86\ISO

    - copy "c:\Program Files\Windows AIK\Tools\amd64\imagex.exe" c:\WinPE_amd64\ISO
    - copy "c:\Program Files\Windows AIK\Tools\ia64\imagex.exe" c:\WinPE_ia64\ISO
- Datei: wimscript.ini erstellen
- Eines der folgenden Commands wählen:
    - oscdimg –n –bc:\WinPE_x86\etfsboot.com c:\WinPE_x86\ISO
    - oscdimg –n –bc:\WinPE_amd64\etfsboot.com c:\WinPE_amd64\ISO
    - oscdimg –n –bc:\WinPE_ia64\etfsboot.com c:\WinPE_ia64\ISO

System Center Configuration Manager (SCCM)

SCCM 2007 ist ein separates Produkt und muss erworben werden.

Wird **SCCM 2007** mit anderen Bereitstellungsmethoden kombiniert, ermöglicht er die Erstellung einer vollständig verwalteten Bereitstellungslösung **für grosse Organisationen**.

Voraussetzungen:
- Auf dem Zielcomputer muss die **Clientsoftware** für den **SCCM 2007** bereits installiert sein.
- Dauerhafte Hochgeschwindigkeitsverbindung zwischen den Servern und den Zielcomputern.

Windows-Aktivierungsinfrastruktur

Mit WVista und W2k8-Server wurde die Volumelizenzbereitstellung dieser Betriebssysteme geändert. Diese müssen innerhalb 30 Tagen nach der Installation aktiviert werden. Damit ist die Aktivierung nun ein integraler Bestandteil der Softwarebereitstellung in grösseren Organisationen.

Es gibt drei **Produktaktivierungsarten**:
- OEM
    - Die OEM-Aktivierung ist eine an das BIOS gebundene automatische Aktivierung.
- Vollprodukt (Retail)
    - Die Vollproduktaktivierung ist die Aktivierung, die Sie durchführen müssen, wenn Sie WVista oder W2k8-Server von einem Softwarehändler gekauft haben.
- Volumen
    - Für Organisationen
    - MAK alle Kunden können einen MAK erwerben.
    - KMS können nur grössere Unternehmen mit mind. 25 WVista und/oder 5 reale W2k8-Server aktivieren.

Eine Volumenlizenzierung unterscheidet zwei Arten von Schlüsseln und drei Aktivierungsmethoden.
- MAK-Schlüssel (Multiple Activation Key)
    - Unabhängige MAK-Aktivierung
    - MAK-Proxyaktivierung
- KMS-Schlüssel (Key Management Service, Schlüsselverwaltungsdienst)
    - KMS-Aktivierung

Bei einer **unabhängigen MAK-Aktivierung** ist der Schlüssel so lange gültig bis eine grössere Hardwareänderung erfolgt. Die Aktivierung wird unterstützt durch das **Volume Activation Management Tool** (VAMT). Das Tool kann von der folgenden Seite heruntergeladen werden:
http://www.microsoft.com/download
Nachdem der **MAK** eingegeben wurde können Sie den Computer mit dem **VAMT** oder über das **Telefon** aktivieren.
Auf einer **Server Core-Installation** erfolgt die Aktivierung mit dem Befehl **slmgr**.

Die **MAK-Proxyaktivierung** kann für Computer eingesetzt werden welche keinen direkten Internetzugang haben.

Die **KMS-Lizenzierung** ermöglicht ohne Kontaktaufnahme mit Microsoft die automatische Aktivierung von Clients in grossen Netzwerken. In einer **KMS-Infrastruktur** gibt es ***nur einen Schlüssel*** im Netzwerk, nämlich den **KMS-Schlüssel**. Dieser Schlüssel wird auf einem einzigen Computer installiert, dem **KMS-Host**, auf dem der **Schlüsselverwaltungsdienst** (Key Management Service, KMS) ausgeführt wird. KMS-Clients versuchen automatisch Verbindung mit einem KMS-Host aufzunehmen und die Aktivierung durchzuführen. Clients, die noch nicht aktiviert sind, versuchen alle 2 Stunden, eine Verbindung mit dem **KMS-Host** herzustellen. Nach erfolgter Aktivierung müssen **KMS-Clients** ihre Aktivierung regelmässig auffrischen. **KMS-Clients** müssen ihre Aktivierung nach spätestens **180 Tagen** erneuern. Aktivierte **KMS-Clients** versuchen alle **7 Tage**, eine Verbindung zum **KMS-Host** herzustellen, und erneuern im Erfolgsfall ihre Aktivierung. Diese gilt dann wieder für **180 Tage**.
Clients, die in diesem Zeitraum nicht aktiviert werden, wechseln in einen ***Modus mit eingeschränktem Funktionsumfang***. Eine KMS-Aktivierung erfordert eine **Mindestanzahl an realen Computern** das bietet einen gewissen Schutz vor Softwarepiraten. Bei der Suche des Clients nach einem **KMS-Host** ist Voraussetzung, dass der KMS-Host ***im DNS über einen SRV-Eintrag*** verfügt.

Wegen der unterschiedlichen Topologien grosser Netzwerke mit vielen Standorten setzen viele ***grosse Organisationen nicht ausschliesslich eine Lizenzierungsart ein***, sondern nach Bedarf beide, **MAK-** und **KMS-Lizenzierung**.

Hypervisor

Type 1 hypervisor:
hypervisors run directly on the system hardware
A “bare metal” embedded hypervisor,

Type 2 hypervisor:
hypervisors run on a host operating system that provides virtualization services, such as I/O device support and memory management.

Hyper-V

Die Virtualisierung wird häufig eingesetzt, um die Arbeitslasten von einer grossen Zahl kaum ausgelasteter realer Server auf einer kleineren Zahl realer Server zusammenzufassen. In Unternehmensnetzwerken liegt die ***Auslastung der realen Server häufig nur bei 5 bis 10 Prozent der Maximalleistung***.

Hyper-V ist eine W2k8-Serverrolle.

Im Gegensatz zu Virtual Server und Virtual PC ist Hyper-V eine **Hypervisor-Technologie**. Ein **Hypervisor** ist eine **dünne Softwareschicht**, die **zwischen Hardware und Betriebssystem** angesiedelt ist. Wenn ein Hypervisor installiert ist, werden Host- und Gastbetriebssysteme in separaten Partitionen installiert, die ***gleichberechtigten Zugriff auf die Hardware*** erhalten.

Im Vergleich zu Virtual PC und Virtual Server bietet Hyper-V deutliche Verbesserung in den Bereichen Leistung, Skalierbarkeit und Verwaltung.

Führen Sie **Domänencontroller** als virtuelle Computer unter **W2k8-Server Hyper-V** aus. Domänencontroller eignen sich ideal für Hyper-V, da sie hauptsächlich Netzwerkdurchsatz- und -verarbeitungsfunktionen für die Verwaltung von Anmeldungen benötigen.

Wandeln Sie die Windows-Installationsmedien in eine **ISO-Datei** um, und stellen Sie diese auf Ihrem Hyper-V-Host zur Verfügung.

Ein virtueller Computer kann einfach auf eine frühere Version (Snapshot) zurückgesetzt werden.

Achten Sie darauf, dass Sie als Netzwerkkarte ***Ältere Netzwerkkarte*** konfigurieren, sonst ist der Adapter nicht **PXE-kompatibel**!

- Unterstützung virtueller Festplattenlaufwerke (vhd-Dateien).
- Erweiterte Gastbetriebssystemunterstützung: Red Hat, SuSe, Solaris, WNT
- Verbesserte Speicherunterstützung bis zu 32 GB/Gast
- Snapshots
- Failoverclusterunterstützung (Test)
- Netzwerklastenausgleich NLB-Farmen
- Keine 64-Bit-Unterstützung für virtuelle Computer
- Bei **Intel-VT** und **AMD-V** wird die Virtualisiserungstechnik HW-Mässig unterstützt
- Mehrkern- und Mehrprozessorunterstützung bis zu vier Prozessoren pro Gast
- Bis zu 4 Netzwerkadapter pro Gast
- SCSI-Unterstützung
- Remoteverwaltung (VMRC)
- Die virtuellen Netzwerkadapter sind standardmässig PXE-fähig
- Unbeschränkte Anzahl von virtuellen Broadcastdomänen

Aktivieren von Hyper-V auf einer **Server Core-Installation**:

```
start /w ocsetup Microsoft-Hyper-V
```

Hyper-V is the server virtualization role in Windows Server 2008. Using Hyper-V, you can run multiple instances of operating systems on a single computer simultaneously. Fewer physical machines help you to reduce costs, increase hardware utilization, and improve server availability. With Hyper-V, you can consolidate servers, enhance business continuity, create safe software test and development environments, and create a dynamic IT environment. You can create and manage a Hyper-V environment by using the basic management tools in Windows Server 2008. Moreover, you can migrate virtual machines from one physical machine to another with minimal downtime.

Clustering in a virtual environment enhances business continuity by transferring applications and services seamlessly between different virtual machines and hosts. You can implement an iSCSI-based storage solution in the cluster to facilitate eight-way clustering that helps in providing better connectivity. Moreover, in Hyper-V, quick migration helps you to rapidly migrate a running virtual machine from one physical host in a cluster to the other.
Hyper-V supports several backup and restore methods. For example, virtual machines can be backed up by running Windows Server Backup in Windows Server 2008. You can also create a snapshot to save the state of a virtual machine at a specified instant.

Hardwarevoraussetzungen

- Viel RAM!
- 64Bit Technologie mit hardwareunterstützter Virtualisiserung (AMD-V oder Intel-VT)
- Datenausführungsverhinderung auf Hardwareebene
  No Execute oder NX-Bit oder Execute Disable XD-Bit

Hyper-V is the hypervisor-based virtualization technology
File Extension: **vmc**

Hyper-V requires specific processor enhancements from either Intel or AMD. Intel VT is supported by XEON 3000, XEON 5000, and XEON 7000 sequence, Intel Itanium 2 processors, and Intel Core 2 processors. These processors generally have a dual-core or quad-core construction.
All AMD Athlon or Opteron processors from revision F2 onwards currently support hardware virtualization and include dual-core and quad-core construction.
Before installing Hyper-V, you need to enable Hardware Data Execution Protection (DEP) in the BIOS. In Intel, DEP is specified by the eXecute Disable (XD) bit. In AMD, it is specified by the No eXecute (NX) bit.
Virtualization is a prime candidate for the expanded memory and processing facilities that 64-bit platforms offer. To ensure these expanded facilities are available, Hyper-V only runs on 64-bit editions of Windows Server 2008.
You can load Windows Server 2008 with Hyper-V on any computer that supports hardware-assisted virtualization. You can also load Hyper-V on all 64-bit platforms that support hardware-assisted virtualization.
Almost all new server hardware is based on a 64-bit platform. Also, there is no difference in the price or licensing for the 64-bit editions of Windows Server 2008. In case you have software that specifically requires a 32-bit environment, you can run the software on a dedicated 32-bit child partition.
Hyper-V is specifically available for the x64-based versions of Windows Server 2008 Standard, Windows Server 2008 Enterprise, and Windows Server 2008 Datacenter.
Physical memory on the host computer is the main limiting factor that determines the number of virtual machines that can run simultaneously. The virtual machines share this physical memory with the parent partition.
Memory requirements are typically 512 MB for the parent partition, the allocated memory for each child partition, and a further 32 MB overhead for each child partition. Therefore, a child partition that has 256 MB of allocated virtual RAM requires a host that has at least (512 + (256 + 32)) = 800 MB of RAM. Hyper-V supports up to 64 GB of RAM for each child partition and up to 2 TB of physical RAM for each host.
A Server Core installation of the Windows Server 2008 operating system is a minimal functionality version of Windows Server 2008 that is controlled through a command-line interface or by using Remote Desktop. You can install Hyper-V on a Server Core installation.
Although it is not necessary to use a Server Core installation for using Hyper-V, it is good practice to do so for improved security, and reduced memory and storage overheads. This makes more memory available for virtual machines.

For more information about Server Core installation, see Server Core Installation of Windows Server 2008 on the Microsoft Web site.

Virtual Server 2005 R2 SP1

- Unterstützung virtueller Festplattenlaufwerke (vhd-Dateien).
- Erweiterte Gastbetriebssystemunterstützung: Red Hat, SuSe, Solaris, WNT
- Failoverclusterunterstützung (Test)
- Netzwerklastenausgleich NLB-Farmen
- Keine 64-Bit-Unterstützung für virtuelle Computer
- Bei **Intel-VT** und **AMD-V** wird die Virtualisiserungstechnik HW-Mässig unterstützt
- Mehrprozessorunterstützung ein Prozessor pro Gast
- Bis zu 4 Netzwerkadapter pro Gast
- SCSI-Unterstützung
- Remoteverwaltung (VMRC)
- Virtual Server 2005 Migration Toolkit (VSMT)
- Die virtuellen Netzwerkadapter sind standardmässig PXE-fähig
- Unbeschränkte Anzahl von virtuellen Broadcastdomänen

Virtual PC 2007

VHD-Dateien werden auch von **Hyper-V** und **Virtual Server** verwendet. Daher lassen sich virtuelle Computer relativ leicht zwischen den Lösungen austauschen.

Die **vhd** kann mit demGratis-Tool **VhdResizer** geschrumpft oder vergrössert werden.
Download: http://vmtoolkit.com

- Unterstützung virtueller Festplattenlaufwerke (vhd-Dateien).
- Keine 64-Bit-Unterstützung für virtuelle Computer
- Bei **Intel-VT** und **AMD-V** wird die Virtualisiserungstechnik HW-Mässig unterstützt
- Einkerniger Prozessor für das Gastsystem
- Bis zu 4 Netzwerkadapter pro Gast
- Die virtuellen Netzwerkadapter sind standardmässig PXE-fähig
- Eine virtuelle Broadcastdomäne für alle Gäste
- Virtual Machine Additions müssen geladen werden

Serverspeicher

Mit dem Aufkommen neuer Technologien wie dem Dienst für virtuelle Datenträger (VDS) und iSCSI sowie mit der zunehmend komplexeren Realität der Datenspeicherung in Unternehmen, gelangt das ehemalige den Spezialisten vorbehaltene Thema (DAS, NAS, SAN) mehr und mehr in den Bereich der Windows Server 2008-Verwaltung.

Direct-Attached Storage (DAS)

DAS ist ein Speicher, der nur an einem einzigen Server angeschlossen ist. Beispiel für eine DAS-Lösung sind die in einem Server eingebauten internen Festplatten oder ein RAID-System, das in einem externen Gehäuse oder Rack eingebaut und über einen SCSI- oder FC-Controller mit einem Server verbunden ist. Der Hauptvorteil eines DAS-Systems ist, dass es einen einzelnen Server mit einem schnellen Speicher auf Blockbasis versorgt, der über einen internen oder externen Bus zugänglich ist (Blockbasis im

Gegensatz zur Dateibasis). DAS ist eine erschwingliche Lösung für Server, die zwar eine gute Leistung, aber keine riesigen Mengen an Speicher bieten müssen.

DAS ist eine gute Lösung für:
- DCs
- DNS-Server
- WINS-Server
- DHCP-Server

Die wichtigste **Beschränkung** von **DAS-Speicher** ist, dass er nur für einen einzigen Server direkt zugänglich ist.
Der **parallele SCSI-Bus** kann maximal **16 Geräte,** mit einer maximalen Entfernung von **25 Metern** verbinden.

Network-Attached Storage (NAS)

NAS ist eigenständiger Speicher, der anderen Servern und Clients im Netzwerk zur Verfügung steht. Ein NAS ist ein vorkonfigurierter Server, auf dem ein Betriebssystem ausgeführt wird, das speziell für Dateidienste entworfen wurde.

Der Vorteil ist, es ist leicht aufzubauen und stellt Clients und Servern eine grosse Menge an Speicherplatz zur Verfügung. Die Verwaltung erfolgt meist mit einem eigenen webbasierten Verwaltungstool.

Der Nachteil von NAS ist natürlich, dass der Zugriff auf ein NAS-Gerät über das Netzwerk erfolgt und nicht über einen lokalen Bus. Daher ist der Zugriff auf die Daten langsamer und erfolgt zudem nicht auf der Basis von Blöcken, sondern auf der Basis von Dateien.

NAS ist eine gute Lösung für:
- Dateiserver
- Webserver
- Server die keine schnellen Datenzugriffe brauchen

Storage-Area Networks (SAN)

Die Hardware sollte unbedingt den **Dienst für virtuelle Datenträger** (VDS) unterstützen, damit eine nahtlose Integration in die Serververwaltung gewährleistet wird.

Sind Hochleistungsnetzwerke, deren Aufgabe es ist, Datenblöcke zwischen Servern und Speichersubsystemen zu transportieren. Aus der Sicht des Betriebssystems sieht SAN-Speicher wie lokaler Speicher aus. Der wichtigste Unterschied zwischen einem SAN und DAS ist der, dass der Speicher bei einem SAN nicht auf einen Server beschränkt ist, sondern einer beliebigen Anzahl von Servern zur Verfügung stehen kann.

Die Hardwaregeräte, die Server und Speicher in einem SAN verbinden, werden auch als **SAN-Fabric** (SAN-System) bezeichnet. Die Geräte werden über Fibre Channel oder Kupferkabel miteinander verbunden. Der verfügbare Speicher wird in **virtuelle Partitionen** (Logical Unit Numbers, LUNs) aufgeteilt und sieht für Server aus wie lokaler Speicher.
SANs haben den Sinn, eine Zentralisierung der Speicherressourcen zu ermöglichen und dabei die Entfernungs- und Verbindungsbeschränkungen aufzuheben, die für DAS gelten.

Die Komponenten einer **SAN-Fabric** sind:
- Hostbusadapter (HBAs)
- Switches
- Festplattensubsysteme
- Bandlaufwerksbibliotheken

SAN ist eine gute Lösung für:

- Server die auf schnelle Datenzugriffe angewiesen sind (Blockbasis)
- Mailserver
- Sicherungsserver
- Streamingmedienserver
- Anwendungsserver
- Datenbankserver
- Replikationsstrukturen

Fibre-Channel-SANs (FC)

Ermöglicht eine Block-Ein- und –Ausgabe mit hoher Leistung. FC basiert auf seriellem SCSI und ist die älteste und am weitesten verbreitete SAN-Verbindungstechnologie. **FC** kann Geräte bis zu einer Distanz von **10 km** verbinden und ermöglichen es eine nahezu unbegrenzte Anzahl von Geräten, über das Netzwerk anzuschliessen. Der Nachteil sind die Kosten der Hardware und die Komplexität der Implementierung.

iSCSI-SANs

Internet-SCSI (iSCSI) ist ein Industriestandard, der zur Übertragung von **SCSI-Blockbefehlen** über ein Ethernetnetzwerk mit dem TCP/IP-Protokoll entwickelt wurde. Server kommunizieren mit iSCSI-Geräten über einen lokal installierten Softwareagenten, der **iSCSI-Iinitiator** genannt wird. Für iSCSI-Fabrics enthält das Netzwerk auch einen oder mehrere **iSNS-Server** (Internet Storage Name Service). iSCSI-SANs sind ***einfacher und preiswerter*** zu implementieren als FC-SANs, haben aber eine geringere Leistung.

iSCSI-SANs haben praktisch keine Einschränkung für den Anschluss von Geräten bezüglich der Distanz. Die Datenübertragung ist gesichert (CHAP/IPSec).

Cluster

In Unternehmensnetzwerken werden häufig mehrere Server zu einer Gruppe zusammengefasst, in der sie dieselben Dienste anbieten.

Unter **W2k8-Server** können Sie drei verschiedene Arten von Servergruppen konfigurieren, um einen Lastenausgelich, gute Skalierbarkeit und hohe Verfügbarkeit zu erreichen. Eine **Round-Robin-Verteilergruppe** ist eine Computergruppe, die DNS verwendet, um mit minimalen Konfigurationsanforderungen einen Lastenausgleich zu erreichen. In einem **NLB-Cluster** (auch NLB-Farm genannt) werden mehrere Server zu einer Gruppe zusammengefasst, um die anfallenden Arbeiten gleichmässig auf die Server zu verteilen und eine gute Skalierbarkeit zu erreichen (NLB steht für Network Load Balancing oder Netzwerklastenausgleich). Ein **Failover-Cluster** schliesslich kann dazu verwendet werden, um auch dann für die Verfügbarkeit einer Anwendung oder eines Dienstes zu sorgen, wenn einer der beteiligten Server ausfällt.

Round-Robin

Beim **Round-Robin** enthält ein **DNS-Server** zur Auflösung eines Servernamens in eine IP-Adresse nicht nur einen Eintrag, sondern mehrere. Wenn Clients den DNS-Server abfragen, um den Namen des Servers aufzulösen ***geht der DNS-Server der Reihe nach diese Einträge durch*** und verweist jeden neuen Client jeweils an eine andere Adresse.
Der Sinn der **Round-Robin-DNS-Abfrage** ist, die Clientabfrage gleichmässig auf die beteiligten Server zu verteilen.
Auf den meisten DNS-Servern wird ***Round-Robin-DNS standardmässig aktiviert***. Um diese einfache Art des Lastenausgleichs zu konfigurieren, brauchen Sie also nur auf dem DNS-Server die entsprechenden DNS-Datensätze zu erstellen.

Der **grösste Nachteil** ist, dass der **DNS-Server** nicht auf den Ausfall eines der beteiligten Server reagiert. Fällt einer der Zielserver aus, verweist der DNS-Server Clients weiterhin an den inaktiven Server, bis ein Netzwerkadministrator den DNS-Eintrag vom DNS-Server löscht.

Netzwerklastenausgleich (NLB)

Network Load Balancing (NLB)

NLB control program: **wlbs.exe**
Befehlszeilentool: **nlbmgr**

NLB ist ein Feature des **W2k8-Servers**.
Für einen Client sieht der **NLB-Cluster** wie ein einziger Server aus. NLB ist eine vollständig verteilte Lösung, die keinen zentralen Verteiler einsetzt.
Ein übliches Szenario ist zum Beispiel der Einsatz von **NLB** bei der Erstellung einer **Webfarm**. Allerdings lässt sich mit **NLB** auch bei der Erstellung einer **Terminalserverfarm**, einer **VPN-Serverfarm** oder eines **ISA-Server-Firewallclusters** verwenden.
Als Mechanismus für den Lastenausgleich bietet **NLB** gegenüber **Round-Robin-DNS** beträchtliche Vorteile. Erstens erkennt **NLB** im Gegensatz zu **Round-Robin-DNS** automatisch, ob ein Server noch mit dem NLB-Cluster verbunden ist oder nicht, und leitet Client anfragen nur an die verbleibenden Server weiter. Ein weiterer Unterschied zwischen NLB und Round-Robin-DNS besteht darin, dass Sie bei NLB den Anteil der Arbeitslast festlegen können, den jeder Host übernehmen soll.

Failover-Cluster

Webcast: www.livemeeting.com/cc/microsoft/view?id=FailoverClustering&pw=josebda

Ein **Failover-Cluster** ist eine Gruppe von zwei oder mehr Computern, die so eingerichtet sind, dass auch beim Ausfall eines Computers möglichst keine Ausfallzeiten für ausgewählte Anwendungen und Dienste entstehen. Die zu einem Cluster zusammengefassten Server werden Knoten genannt. ***Sie werden mit Kabel untereinander und mit dem gemeinsamen Speicher verbunden***.
Die Server eines Failover-Clusters können verschiedene Rollen übernehmen, beispielsweise die Rolle als **Datei-, Druck-, E-Mail-** oder **Datenbankserver**.
In den meisten Fällen gehört zu einem Failover-Cluster ein gemeinsames Speichergerät, das direkt mit allen Servern des Clusters verbunden ist, wobei allerdings jedes Volume des Speichers zu jedem Zeitpunkt immer nur von einem Server verwendet wird.

Installation:

1. Der erste Schritt ist die **Installation der Hardware**
2. Dann müssen Sie das **Feature Failover-Clusterunterstützung** installieren
3. Dann das **Failover-Cluster Validation Tool** ausführen um zu überprüfen ob die HW- und SW-Voraussetzungen erfüllt sind
4. Dann wird der Cluster mit dem **Clustererstellungsassistenten** erstellt.
5. Um das Verhalten des Clusters genau einzustellen müssen Sie den Assistenten für **hohe Verfügbarkeit** ausführen

Die **Quorumkonfiguration** in einem Failover-Cluster bestimmt die Anzahl der Ausfälle, die im Cluster auftreten dürfen, bevor der Cluster insgesamt ausfällt. Getestet wird der **Failover**, indem der Dienst oder die Anwendung in einen anderen Knoten verschoben wird.

- Knotenmehrheit
- Knoten- und Datenträgermerheit
- Knoten- und Dateifreigabemehrheit
- Keine Mehrheit: Nur Datenträger

Netzwerkübersicht

Ein ***Netzwerkbroadcast*** ist eine Übertragung, die sich an alle lokalen Adressen richtet. Ein solcher ***Broadcast*** wird durch alle ***Schicht 1-*** und ***Schicht 2-Geräte*** (Kabel, Repeater, Hubs, Bridges und Switches) transportiert, aber von ***Schicht 3-Geräten*** (Routern) blockiert.

Computer die miteinander über ***Broadcast*** kommunizieren können liegen in der derselben ***Broadcastdomäne***.

Die ***alternative Konfiguration*** ist besonders für mobile Computer nützlich.

Link Layer Topology Discovery LLTD (Muss auf WXP installiert werden!).

Programm: **rspndr.exe**
Dienst starten: **net start rspndr**

Rollen

Active Directory-Zertifikat Server (AD CS)

Windows Remote Management

Befehlszeilentools:
winrm.cmd (API)
winrs.exe (Remote Ausführung von cmd.exe)

Netzwerk-Bridge

Verbindet im Computernetz zwei Segmente auf der Ebene der Schicht 2 (Sicherungsschicht) des OSI-Modells. Eine Bridge kann auf der Unterschicht MAC oder der Unterschicht LLC arbeiten. Sie wird dann **MAC-Bridge** oder **LLC-Bridge** genannt. Eine weitere Unterscheidung ergibt sich durch die Art der Leitwegermittlung von Datenpaketen in **Transparent Bridge** und **Source Routing Bridge**.

Windows CardSpace

(ehemals InfoCard) ist Bestandteil des Microsoft .NET Frameworks. CardSpace ist eine Technologie zur ***Identitätsverwaltung*** und kann zur ***Authentifizierung*** und/oder ***Identifizierung*** gegenüber Webseiten und Webservices genutzt werden. Unter Windows Vista wird CardSpace mitgeliefert, bei Windows XP kann es nachträglich installiert werden, indem auf die letzte .NET Framework Version aktualisiert wird. Für andere Betriebssysteme wie Apples Mac OS X oder Unix-Derivate gibt es alternative Implementierungen, welche meistens mit dem Begriff ***Information Card*** oder ***InfoCard*** bezeichnet werden.
Die CardSpace-Technologie soll es dem Endanwender (und auch Mitarbeitern in Firmen) erleichtern, die eigene Identität gegenüber Dritten (Relying Party) zu versichern. Bisher ist es normalerweise so, dass man sich z. B. auf einer Webseite mit einem Benutzernamen und einem Passwort anmeldet (z. B. bei einem Webmail-Anbieter). Diese Methode ist fehleranfällig und unsicher, da die Mehrzahl der Benutzer unsichere Passwörter nutzt oder die Passwörter über eine unverschlüsselte, also unsichere Leitung geschickt werden.

Zur ***Migration*** der Sicherheitsinformationen, die Applikation **"Windows CardSpace"** verwenden.

New TCP/IP-Stack

Bessere Performance.

IP

Adressbereiche

Private Adressbereiche

10.0.0.0	-	10.255.255.254
172.16.0.0	-	172.31.255.254
192.168.0.0	-	192.168.255.254

Private IP-Adressen können nicht in das öffentliche Internet geroutet werden.

Berechnung der Hostkapazität

Adressblock (/ 24) = 256 Adressen
0 = NetzID
255 = Broadcastadresse des Subnetzes

Das Netzwerk 192.168.10.0/24 hat Platz für 256 Adressen.
Die Adresse 192.168.10.0 ist für die NetzID reserviert
Die Adresse 192.168.10.255 ist die Netzwerkbroadcastadresse.
Somit bleiben 254 Adressen übrig, die an Netzwerkhosts zugewiesen werden können.

Gebräuchliche Adressblöcke

CIDR	Punk-Dezimal Notation	Adressen	Hosts(-2)
/20	255.255.240.0	5096	5094
/21	255.255.248.0	2048	2046
/22	255.255.252.0	1024	1022
/23	255.255.254.0	512	510
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2

Berechnung der Subnetze

Subnetze = 2^b
$b = n_{int} - n_{ext}$

Beispiel:
Zugeteilter Adressblock: 10.10.100.0/24 ($n_{ext} = 24$)
Verwendete Subnetmaske: 10.10.100.0/27 ($n_{int} = 27$)
$b = 27 – 24 = 3$
Anzahl Subnetze = 2^3 = **8**

Subnetmasken variabler Länge (VLSM-Technik)

Auftrag: Subnetz A mit 100 Hosts
Subnetz B mit 50 Hosts
Subnetz C mit 20 Hosts
Adressblock: 10.41.1.0/24
Resultat: Subnetz A = 10.41.1.0/25
Subnetz B = 10.41.1.128/26
Subnetz C = 10.41.1.192/27

CIDR	Punk-Dezimal Notation	Subnetze	Adressen	Hosts (Adressen-2)	
/24	255.255.255.0	1	256	254	11111111 11111111 11111111 00000000
/25	255.255.255.128	2	128	126	11111111 11111111 11111111 10000000
/26	255.255.255.192	4	64	62	11111111 11111111 11111111 11000000
/27	255.255.255.224	8	32	30	11111111 11111111 11111111 11100000
/28	255.255.255.240	16	16	14	11111111 11111111 11111111 11110000
/29	255.255.255.248	32	8	6	11111111 11111111 11111111 11111000
/30	255.255.255.252	64	4	2	11111111 11111111 11111111 11111100

Broadcastbereich

Ein Host kann ine IP-Adresse von einem ***DHCP-Server*** erhalten, wenn ein ***DHCP-Server*** oder ***DHCP-Relay-Agent*** innerhalb des ***Broadcastbereichs*** liegt.

NETSH-Befehl

```
netsh interface ip set address <Verbindungsname> static <Adresse> <Subnetzmaske>
(<Standardgateway>)

netsh interface ip set address "LAN-Verbindung" static 10.41.1.10 255.255.255.0

netsh interface ipv6 show interface
```

DHCP-Infrastruktur

Dynamic Host Configuration Protocol.

Mac-Adressen abfragen: **getmac**

DHCP-Adresszuweisung

1. DHCP-Discover Broadcast (Client)
2. DHCP-Offer vom (Server)
3. DHCP-Request (Client)
4. DHCP-Ack (Server)

DHCP Optionen

- 003 Router Standardgateway
- 006 DNS
- 015 DNS Servers. Kann beliebig viel DNS-Einträge enthalten.
- 044 WINS/NBNS Servers
- 045 NetBIOS oder NetBIOS-über TCP/IP Fehler! Textmarke nicht definiert.over TCP/IP NBDD
- 046 WINS/NBT Node Type
- 051 Lease auf 1 - max. 3 Tage stellen!

Achtung! DHCP muss **autorisiert** werden!

Adressausschlüsse, Reservierungen, Leasedauer
Optionen für: Server-, Bereichs-, und Reservierungsebene

IPv6

Eine IPv6-Adresse müssen Sie üblicherweise nicht von Hand zuweisen, weil statische IPv6-Adressen üblicherweise nur an ***Router*** vergeben werden, nicht an Hosts.

Hosts erhalten Ihre IPv6-Adresse von benachbarten ***Routern*** oder von ***DHCPv6-Servern***.

```
ipconfig /renew6
```

Adressraum: 2^{128} = 340 Sextillionen (3.4×10^{38})

Acht Blöcke à vier Hexadezimalziffern: `AAAA:BBBB:CCCC:DDDD:1111:2222:3333:4444`

- Führende Nullen werden bei der Schreibweise weggelassen: `00FA` ➔ `FA`
- Aufeinanderfolgende Null-Blöcke als :: schreiben:
  `FA:0000:0000:0000:0000:3FA9:D3:9C5A` ➔ `FA::3FA9:D3:9C5A`
- Loopback-Adresse: `::1`
- IPv6-Multicastadresse auf (**`FF02::1:3`**) ➔ für LLMNR

Unicast, Multicast und Anycast

64 Bit NetzwerkID + 64 Bit HostID

Unicast bedeutet, dass eine Nachricht an ein einziges Ziel gesendet wird.
Multicast bedeutet, wird an mehrere Ziele gesendet und Anycast beduete es wird an einen beliebigen Computer gesendet.

Globale Adressen

Gegenstück zu IPv4 ***Öffentlichen-Adressen***.

Wert zwischen: **`2000 - 3FFF`** **`oder`** **`2000::/3`**

Aufteilung: 48 Bit(Öffentliches Routing) 16 Bit(Privates Routing) 64 Bit Hostkennung)

Verbindungslokale Adressen

Auch: Link-Local Address (LLA)

Gegenstück zu IPv4 ***APIPA-Adressen***.

Präfix: **`FE80`**

Enthält am Schluss die Zonen-ID (%ID)

Aufteilung: 64 Bit(Nicht routingfähige NetID) 64 Bit Hostkennung) %99 (ZonenID)

Eindeutige lokale Adressen

Wert zwischen: **`FD00 - FDFF`**

Gegenstück zu IPv4 ***Privaten-Adressen*** (10…/ 172…/ 192…)

Standortlokale Adressen

Wert zwischen: **`FD00 - FDFF`**

Präfix: **FEC0/10**

ISATAP

Technik damit ein reines IPv4-LAN mit einem reinen IPv6-LAN kommunizieren kann.

6to4

Technik, damit ein IPv4-Host mit einem IPv6-LAN kommunizieren kann

Teredo

Mithilfe von Teredo können Hosts, die hinter einem **IPv4-NAT** liegen, über **IPv6** miteinander oder mit reinen IPv6-Hosts im Internet kommunizieren. Erlaubt Peer-to-Peer Communication zwischen Branch Offices.

Configuring IPv6 With the Netsh.exe Tool

In the same way as IPv6 for Windows XP, you can configure IPv6 addresses and other configuration parameters at the command line using commands in the **netsh interface ipv6** context.

Configuring Addresses

To configure IPv6 addresses, you can use the **netsh interface ipv6 add address** command with the following syntax:

netsh interface ipv6 add address [**interface=**]*Interface_Name_or_Index*
[**address=**]*IPv6_Address*[**/***Prefix_Length*] [[**type=**]**unicast**|**anycast**] [[**validlifetime=**]*Time*|**infinite**]
[**preferredlifetime=**]*Time*|**infinite**] [[**store=**]**active**|**persistent**]

- **interface** The connection or adapter's name or interface index.
- **address** The IPv6 address to add, optionally followed by the subnet prefix length (default of 64).
- **type** The type of IPv6 address, either unicast (default) or anycast.
- **validlifetime** The lifetime over which the address is valid. Time values can be expressed in days, hours, minutes, and seconds, for example 1d2h3m4s. The default value is infinite.
- **preferredlifetime** The lifetime over which the address is preferred. Time values can be expressed in days, hours, minutes, and seconds. The default value is infinite.
- **store** How to store the IPv6 address, either active (the address is removed upon system restart) or persistent (address remains after system restart) (default).

For example, to configure the IPv6 unicast address 2001:db8:290c:1291::1 on the interface named "Local Area Connection" with infinite valid and preferred lifetimes and make the address persistent, you would use the following command:

```
netsh interface ipv6 add address "Local Area Connection"
2001:db8::290c:1291::1
```

Adding Default Gateways

To configure a default gateway, you can use the **netsh interface ipv6 add route** command and add a default route (::/0) with the following syntax:

netsh interface ipv6 add route [**prefix=**]**::/0** [**interface=**]*Interface_Name_or_Index*
[[**nexthop=**]*IPv6_Address*] [[**siteprefixlength=**]*Length*] [[**metric=**]*Metric_Value*]

[[**publish=**]**no**|**yes**|**immortal**] [[**validlifetime=**]*Time*|**infinite**] [[**preferredlifetime=**]*Time*|**infinite**] [[**store=**]**active**|**persistent**]

- **prefix** The IPv6 address prefix and prefix length for the default route. For other routes, you can substitute ::/0 with *Address_Prefix***/***Prefix_Length*.
- **interface** The connection or adapter's name or interface index.
- **nexthop** If the prefix is for destinations that are not on the local link, the next-hop IPv6 address of a neighboring router.
- **siteprefixlength** If the prefix is for destinations on the local link, you can optionally specify the prefix length for the address prefix assigned to the site to which this IPv6 node belongs.
- **metric** A value that specifies the preference for using the route. Lower values are more preferred.
- **publish** As an IPv6 router, this option specifies whether the subnet prefix corresponding to the route will be included in router advertisements and whether the lifetimes for the prefixes are infinite (the **immortal** option).
- **validlifetime** The lifetime over which the route is valid. Time values can be expressed in days, hours, minutes, and seconds, for example 1d2h3m4s. The default value is infinite.
- **preferredlifetime** The lifetime over which the route is preferred. Time values can be expressed in days, hours, minutes, and seconds. The default value is infinite.
- **store** How to store the route, either active (route is removed upon system restart) or persistent (route remains after restart) (default).

For example, to add a default route that uses the interface named "Local Area Connection" with a next-hop address of fe80::2aa:ff:fe9a:21b8, you would use the following command:

```
netsh interface ipv6 add route ::/0 "Local Area Connection"
fe80::2aa:ff:fe9a:21b8
```

Adding DNS Servers

To configure the IPv6 addresses of DNS servers, you can use the **netsh interface ipv6 add dnsserver** command with the following syntax:

netsh interface ipv6 add dnsserver [**interface=**]*Interface_Name_or_Index* [[**address=**]*IPv6_Address*] [[**index=**]*Preference_Value*]

- **interface** The connection or adapter's name or interface index.
- **address** The IPv6 address of the DNS server.
- **index** The preference for the DNS server address.

  By default, the DNS server is added to the end of the list of DNS servers. If an index is specified, the DNS server is placed in that position in the list and the other DNS servers are moved down the list.

For example, to add a DNS server with the IPv6 address 2001:db8::99:4acd::8 that uses the interface named "Local Area Connection," you would use the following command:

```
netsh interface ipv6 add dnsserver "Local Area Connection"
2001:db8::99:4acd::8
```

Disabling IPv6

Unlike Windows XP, IPv6 in Windows Vista cannot be uninstalled. However, you can disable IPv6 in Windows Vista by doing one of the following:

- In the Connections and Adapters folder, obtain properties on all of your connections and adapters and clear the check box next to the Internet Protocol version 6 (TCP/IPv6) component in the list under **This connection uses the following items**. This method disables IPv6 on your LAN interfaces and connections, but does not disable IPv6 on tunnel interfaces or the IPv6 loopback interface.

- Add the following registry value (DWORD type) set to 0xFFFFFFFF:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\DisabledComponents
  This method disables IPv6 on all your LAN interfaces, connections, and tunnel interfaces but does not disable the IPv6 loopback interface. You must restart the computer for this registry value to take effect. DisabledComponents is set to 0 by default.

The DisabledComponents registry value is a bit mask that controls the following series of flags, starting with the low order bit (Bit 0):

1. **Bit 0** Set to 1 to disable all IPv6 tunnel interfaces, including ISATAP, 6to4, and Teredo tunnels. Default value is 0.
2. **Bit 1** Set to 1 to disable all 6to4-based interfaces. Default value is 0.
3. **Bit 2** Set to 1 to disable all ISATAP-based interfaces. Default value is 0.
4. **Bit 3** Set to 1 to disable all Teredo-based interfaces. Default value is 0.
5. **Bit 4** Set to 1 to disable IPv6 over all non-tunnel interfaces, including LAN interfaces and Point-to-Point Protocol (PPP)-based interfaces. Default value is 0.
6. **Bit 5** Set to 1 to modify the default prefix policy table to prefer IPv4 to IPv6 when attempting connections. Default value is 0.

To determine the value of DisabledComponents for a specific set of bits, construct a binary number consisting of the bits and their values in their correct position and convert the resulting number to hexadecimal. For example, if you want to disable 6to4 interfaces, disable Teredo interfaces, and prefer IPv4 to IPv6, you would construct the following binary number: 101010. When converted to hexadecimal, the value of DisabledComponents is 0x2A.
You must restart the computer for the changes to the DisabledComponents registry value to take effect.

Namensauflösung

1. DNS
2. LLMNR
3. NetBIOS

Dynamische DNS-Server (DDNS)

DDNS-Server sind schreibgeschützte Server, aber sie akzeptieren nur Registrierungen von bekannten Entitäten. Intelligente Geräte, wie z.B. Computer unter W2k, WXP, W2k3, WVista und W2k8 können eigene Namen in einem DDNS registrieren.

DSN-Server mit Schreibzugriff

Die gängigste Art des DNS-Servers mit Schreibzugriff ist der **primäre DNS-Server**. **Primäre DNS-Server** werden üblicherweise in Umkreisnetzwerken bereitgestellt. und nicht in AD DS integriert.

Schreibgeschützte DNS-Server

DNS-Server die eine schreibgeschützte Kopie der DNS-Daten enthalten, die von einem anderen Standort stammen. Es wird ausschliesslich eine einseiteige Replikation unterstützt.

Split-Brain Syndrom

Wenn Sie für ihre AD DS-Verzeichnisstruktur intern denselben Namen verwenden wie zur externen Darstellung im Internet, müssen Sie einen sogenannten Split-Brain-DNS-Dienst implementieren.

Whole-Brain

Round-Robin

DNS-Dienste können zur Bereitstellung einer Art Hochverfügbarkeit genutzt werden. Dies wird erreicht, indem mehrere Einträge für dieselbe Ressource erstellt werden., die jeweils eine andere IP-Adresse aufweisen. Damit kann die Last auf mehrere Server verteilt werden.

Die Standardeinstellung für Round-Robin-Rotation ist im Registrierungseintrag **RoundRobin** (REG_DWORD) enthalten

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DNS\Parameters
```

Der Registrierungseintrag **DoNotRoundRobinTypes** (REG_SZ) mit einem Zeichenfolgenwert enthält eine Liste mit RR-Typen. Durch Ändern dieses Eintrags können Sie die Round-Robin-Rotation für bestimmte RR-Typen deaktivieren.

Web Proxy Automatic Discovery Protocol (WPAD)

Das **Protokoll**, das Webbrowser zur Ermittlung der Proxyeinstellungen für das Netzwerk nutzen.

Footprinting

Wenn ein Angreifer versucht, alle Daten in einem DNS-Server abzurufen, um anhand dieser Daten die im Netzwerk enthaltenen Objekte zu identifizieren.

NetBIOS oder NetBIOS-über TCP/IP

Aktivieren/Deaktivieren: Netzwerkeinstellungen Registerkarte WINS.

Kann mit einer Gesellschaft verglichen werden, in der es nur einen Vornamen, der einmal vorkommt und keine Nachnamen gibt.

- NetBIOS ist inkompatibel zu ***IPv6***.

- NetBIOS umfasst 3 Namensauflösungsmethoden: ***Broadcast***, ***WINS***, und ***LMHOSTS***.
- Mit ***WINS*** und ***LMHOSTS*** kann die Namensauflösung über das lokale Subnetz hinaus erweitert werden.

NetBIOS-Knotentypen

- B-Knoten / Broadcast
- P-Knoten / Punkt-zu-Punkt (WINS)
- M-Knoten / B- dann P-Knoten
- H-Knoten / Hybrid (WINS -> LMHOST -> Broadcast) ➔ Standard

WINS

Falls der WINS-Server benötigt wird, installieren Sie WINS auf **mindestens zwei Servern**.
Beachten Sie, dass WINS auf W2k8 **keine Rolle** sondern ein **Feature** ist.
Bei mehreren WINS-Server am besten Push-Pull-Replikation verwenden.
Im Bestreben, diesen früheren Dienst aus Windows basierten Netzwerken zu entfernen, hat Microsoft in W2k8-Server die **globale Namenszone** (GlobalNames Zone, GNZ) in **DNS** implementiert. **GNZ kannWINS ersetzen**.

LMHOSTS

%SystemRoot%\System32\Drivers\Etc

GlobalNames-Zone (GNZ)

Wenn Sie Namen mit einer einzigen Bezeichnung verwalten möchten, müssen Sie manuell eine globale Namenszone (GNZ) erstellen.
Die Konfiguration erfolgt über den Befehl: **dnscmd.exe**

Link Local Multicast Name Resolution (LLMNR)

Aktivierung über ***Netzwerkerkennung***.
Deaktivierung über Gruppenrichtlinien:
Computerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\DNS-Client <Multicastnamensauflösung>

- Löst nur Namen im lokalen Subnetz auf.
- Löst Namen durch senden der IPv6-Multicastadresse auf (`FF02::1:3`)
- 224.0.0.252 IPv4 Namensauflösungsanforderung durch LLMNR
- Wird nur durch Windows Vista und Windows Server 2008 es werden keine ältere Windows Versionen unterstützt.
- Wenn keine DNS-Infrastruktur zur Verfügung steht.
- Wenn LLMNR zur Verfügung steht wird es vor NetBIOS verwendet.

Peer Name Resolution (PNRP)

Da sowohl **W2k8-Server** als auch **WVista** vollständige Unterstützung für **IPV6** bieten, bieten diese zwei Betriebssysteme ein sekundäres System für die Namensauflösung, das **Peer Name Resolution Protocol** (PNRP). Im Gegensatz zu **DNS**, das auf einer **hierarchischen Namensstruktur** aufbaut, basiert **PNRP** auf **Peersystemen** zum Auflösen des Standortes eines Computersystems. Im Grunde ist PNRP ein **Referenzierungssystem**, das **Suchläufe** basierend auf bekannten Daten durchführt. Wenn Sie beispielsweise nach Computer A suchen und Sie sich in der Nähe von Computer A und C befinden, fragt Ihr System Computer B, ob ihm Computer A bekannt ist. Wenn Computer B dies bejaht, wird eine Verbindung zu Computer A bereitgestellt.

- Es handelt sich um ein verteiltes Namenssystem, das sich zum Auffinden von Objekten nicht auf einen zentralen Server verlässt.
- PNRP kann Milliarden von Namen verwalten
- PNRP ist fehlertolerant

- Die Namensveröffentlichung erfolgt sofort, ist kostenfrei und erfordert keinerlei administrativen Eingriffe wie bei DNS.
- Namen werden in Echtzeit aktualisiert
- Unterstützt die Benennung von Diensten und Computern
- PNRP-Namen können durch digitale Signaturen geschützt werden

Routing

Während das Paket zwischen Netzwerken weitergeleitet wird, ändern sich Quell- und Ziel-IP-Adressen niemals. Die Quell- und Ziel-MAC-Adressen jedoch werden für jedes Nwtzerk zwischen und Server neu eingetragen.

Das verwendete ***Routingprotokoll*** bei W2k8 ist RIP V2.

```
route –p add <NetzID> MASK 255.255.255.0 <Gateway>
```

IPSec

IPSec ist im wesentlichen ein Mechanismus, um Sicherheit für die Daten zu gewährleisten, die zwischen zwei Computern in einem IP-Netzwerk ausgetauscht werden. Weil IPSec ein Standard ist, der Interoperabilität bietet, kann IPSec verwendet werden, um die Kommunikation zwischen Windows und Nicht-Windows-Computern zu schützen.

Datenauthentifizierung, Datenintegrität, Verschlüsselung.

Filteraktionen: Blocken, zulassen oder "Sicherheit aushandeln".

Kerberos ist das Standardauthentifizierungsprotokoll in einer Active Directory-Umgebung.
Zertifikate: Empfohlen wenn keine Kerberos-Authentifizierung verfügbar ist.
Vorinstallierte Schlüssel: Nicht empfohlen!

Sicherheitszuordnungen

Security Association(SA).

- Authentication Header(AH)
  Bietet Authentifizierung
- Encapsulating Security Payload(ESP)
  Bietet: Authentifizierung und Datenveschlüsselung.

Um SA's dynamisch zwischen IPSec-Partnern aufzubauen, wird das ***IKE-Protokoll*** (Internet Key Exchange) benutzt.

IKE wird in zwei Phasen aufgebaut:

- Phase 1: main mode
- Phase 2: quick mode

Network Adress Translation (NAT)

Wird verwendet, damit Hosts, die private IP-Adressen haben, im Internet kommunizieren können. Dabei werden private IP-Adressen, durch einen NAT-Server in öffentliche IP-Adressen übersetzt.

- Wegen des grösseren Adressraums und der besseren Architektur für private Adressierung wird NAT von IPv6 nicht benötigt.
- Dedizierte Hardware ist die bessere Wahl für einen NAT-Server. Viele Router haben NAT-Fähigkeiten integriert.

Remote Desktop Protocol (RDP) läuft über **TCP-Port 3389**

W2k8(enthält zwei NAT-Dienste
- Internet Connection Sharing (ICS)
- Routing und RAS-Dienste

Internet Connection Sharing (ICS)

- Die interne Netzwerkschnittstelle hat immer die IP-Adresse ***192.168.0.1***.
- Es wrid automatisch ein ***DHCP-Dienst*** aktiviert, der Adressen aus dem ***Raum 192.168.0.0/24*** zuweist.
- Dieser DHCP-Dienst ist nicht kompatibel mit den ***DHCP-Server*** und ***DHCP-Relay-Agent*** Rollen des W2k8-Servers.

Routing und RAS-Dienste (RRAS)

Vorteile gegenüber ICS:
- Es können andere interne Netzwerke als 192.168.0.0/24 verwendet werden.
- Sie können Routen in mehrere Netzwerke eingerichtet werden.
- Es können andere DHCP-Serevr verwendet werden.

Drahtlosnetzwerke

Public Key Infrastructure (PKI)

Wi-Fi-Protected Access (WPA)
WPA2-EAP (Extensible Authentication Protocol)
WPA-EAP (Extensible Authentication Protocol)
WPA2-PSK (Pre Shared Key)
WPA-PSK (Pre Shared Key)

Wired Equivalent Protection (WEP)
126-Bit WEP
64-Bit WEP

802.11 Vorläufer von 802.11b wurde aber nie auf breiter Ebene eingesetzt.
802.11a Verwendet 5.4GHz Bereich statt 2.4GHz-Bereich (fast völlig veschwunden)
802.11b 11MBit/s (praktisch 3-4MBit/s)
802.11g 54MBit/s (praktisch 10-15MBit/s)
802.11n 250MBit/s (praktisch ???)

Infrastrukturmodus: Verwendet einen Drahtloszugriffspunkt (Access-Point).
Ad-Hoc-Netzwerk: Peer-to-Peer.

Netzwerkzugriffsschutz (Network Access Protection, NAP)

Rolle: Netzwerkrichtlinienserver (Network Policy Server, NPS)
NPS ist die Microsoft-Implementierung eines RADIUS-Servers und -Proxys.
Remote Authentication Dial-In Service (RADIUS)

Extensible Authentication Protocol (EAP): Wurde als Erweiterung des PPP entwickelt und erlaubt neuere Authentifizierungs-Methoden wie Einmaliges Passwort (one-time password), smart-cards und Biometrische Techniken.

Protected Extensible Authentication Protocol (PEAP)
PEAP-MSCHAPv2

Remotenetzwerke

DFÜ-Verbindungen

Vorteile:
- Keine Internetverbindung nötig
- Minimales Datenschutzrisiko
- Konstante Leistung

Nachteile:
- Hohe Kosten für Skalierbarkeit
- Geringe Bandbreite

VPN-Verbindungen

Vorteile:
- Hohe Bandbreite möglich
- Geringe Kosten

Nachteile:
- Intdernetverbindung nötig
- Schlechte Latenz
- Schlechte Effizienz bei DFÜ-Verbindung

Braucht zwei Netzwerkkarten.

W2k8(-Server unterstützt drei VPN-Technologien:
- PPTP (Point-to-Point Tunneling Protocol)
- L2TP (Layer Two Tunneling Protocol)
  z.B. L2TP/IPSec + EAP-TLS Authentifizierung(Zertifikatbasiert)
- SSTP (Secure Socket Tunneling Protocol)

Secure Socket Tunneling Protocol (SSTP)
- Wird nur von W2k8-Server und WVista SP1 unterstützt.
- Transportiert PPP Verkehr durch einen SSL-Kanal.

Windows Firewall & Netzwerkzugriffsschutz (NAP)

Firewallprofile
- Domäne
- Privat
- Öffentlich

RAS Error 721 ➔ Generic Route Encapsulation (GRE)
- Release Port 1723 on Firewall

Network Access Protection (NAP)

NAP arbeitet mit einem NAP-Integritätsrichtlinienserver (W2k8-Server) der als RADIUS-Server agiert.

Wenn Sie NAP als Schutz gegen böswillige Angreifer betrachten, dürfen Sie nicht vergessen, dass NAP darauf vertraut, dass der ***Systemintegritätsagent (System Health Agent, SHA)*** die Systemintegrität des Clients ehrlich meldet (Signiertes "Statement of Health", ***SoH***). Der ***SHA*** läuft auf dem Clientcomputer!

Statement of Health (SoH)
System Health Validator (SHV)
Statement of Health Response (SoHR)
Health Registration Authority (HRA)

NAP kann Hosts, welche die Integritätsanforderungen nicht erfüllen in einem Netzwerk isolieren (Wartungsnetzwerk, remediation network), wo sie z.B. Updates herunterladen oder Antivirensoftware installiert wird. Hierzu wird das NAP Client Configuration Tool eingesetzt.

Die Implementation eines NAP sollte in 3 Schritten erfolgen

1. Test
2. Überwachung
3. Aktivierung mit eingeschränktem Zugriff

NP Erzwingungstypen

- IPSec-Verbindungssicherheit
- 802.1X-Zugriffspunkt
  Standard zur Authentifizierung und Autorisierung in Rechenzentren.
  - ACL
  - VLAN
- VPN-Server
- DHCP-Server

Policies

- Connection Request Policy
- Network Policy

Examples:

Policy name	Policy condition	Troubleshooting URL	Processing order
ABC Compliant	Health Policy: Pass A, B, C	N/A	1
ABC Noncompliant	Health Policy: Fail A, B, C	http://NAP/abc.html	2
AB Noncompliant	Health Policy: Fail A, B	http://NAP/ab.html	3
AC Noncompliant	Health Policy: Fail A, C	http://NAP/ac.html	4
BC Noncompliant	Health Policy: Fail B, C	http://NAP/bc.html	5
A Noncompliant	Health Policy: Fail A	http://NAP/a.html	6
B Noncompliant	Health Policy: Fail B	http://NAP/b.html	7
C Noncompliant	Health Policy: Fail C	http://NAP/c.html	8
Non NAP-capable	NAP-Capable: Non NAP-capable	N/A	9

Abbildung 11: Policy Names

Windows Security Health Validator

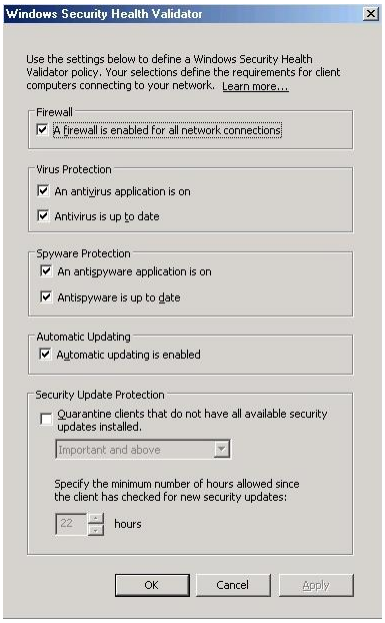


Abbildung 12: Windows Security Health Validator

Bootstrap Wireless Profile
Temporäres Wireless start Profil, um den Client an einer Sicheren Domäne anzumelden.

Windows Server Update Services (WSUS)

Mit WSUS können sie MS-Updates herunterladen, genehmigen und in Ihrer Organisation verteilen.
Es lässt sich über Gruppen steuern, welche Computer welche Updates erhalten.
Durch eine geschickte Update-Architektur verschiedener WSUS-Server kann die benötigte Bandbreite minimiert werden.

Das verwendete Protokoll für WSUS ist ***HTTP***.

Upstreamserver: Bedient Downstreamservers.
Downstreamserver: Holt die Updates von einem Upstreamserver ab.

Download von WSUS: http://www.microsoft.com/wsus

Nicht unterstützte Clients: **WXP , W2k**

MS System Center Configuration Manager 2007
Download: http://www.microsoft.com/smserver

MS Baseline Security Analyzer (MBSA)
Download: http://www.microsoft.com/mbsa

Windows Update Dienst

net start wuauserv
net stop wuauserv

wuauclt /a (Windows update sofort starten)

Ereignissweiterleitung

Bei WVista, W2k8-Server und W2k3-Server R2 können Sie mithilfe von Ereignissweiterleitung (event forwarding) Ereignisse von Remotecomputern sammeln und Probleme feststellen bevor es richtig Ernst wird.

Die Ereignissweiterleitung verwendet das Protokoll: ***HTTP*** oder ***HTTPS***

Sammelcomputer

Konfiguration: **wecutil qc**

Voraussetzungen:

- Abonnement erstellen
- Sammlungsinitiiert
- Quellcomputerinitiiert

Windows Event Collector Utility

```
wecutil ss <Abonnementname> /cm:custom
wecutil ss <Abonnementname> /hi:12000

wecutil gs "Abonnementname"
```

Windows Remote Shell

```
winrm get winrm/config

winrm quickconfig –transport:https
```

Weiterleitungscomputer

Voraussetzungen:

- Dienst: Windows-Remoteverwaltung
- Dienst: Windows-Ereignisssammlung
- Firewallausnahme für http
- `net localgroup "Ereignisprotokollleser" <server>@<domain>`

Konfiguration: **winrm quickconfig** oder **winrm qc**

Aktivieren der Remoteverwaltung über GPO

```
Computerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\Netzwerkverbindungen\Windows-Firewall\Domänenprofil
Option: Windows-Firewall\Eingehenden Remoteverwaltungsausnahme zulassen
```

Überwachung

Systemmonitor

Leistungsindikator auswählen: Ctrl + H (Wird schwarz und Fett angezeigt)

Zuverlässigkeitsüberwachung/RACAgent

Reliability Analysis Component: **racagent.exe**

- Stabilitätsindex 10 am besten.
- Der Task Scheduler muss gestartet sein!

Sammlungssätze

Network Monitor

Kostenloser Protokoll-Analyzer.
Download: http://www.microsoft.com/downloads (Suchen nach: "Network Monitot")

Treiber wird für jede Schnittstelle installiert ("Microsoft Network Monitor 2-Driver")

"promiscuous mode" oder "monitor mode"

Nützliche Daten: "Frame Details"

Filter einsetzen.
Filter können zur Eingrenzung mit && und || kombiniert werden

Verwalten von Dateien

W2k8-Server Rolle: Dateidienste

DFS, Ressourcen-Manager, NFS, Windows Suchdienst und W2k3 Dateidienste

NTFS

NTFS-Dateiberechtigung
Kontingente beeinflussen die Datenträgerleistung nur unwesentlich.
Befehlszeilentool: **dirquota /?**

- Benutzerdateien
- Systemdateien
- Programme

NTFS-Encryption

- Public Key
- Digital Certificates

Encrypting File System (EFS)

Verschlüsseln von Ordnern und Dateien
Die Datenträgerleistung wird um 10 – 60% verschlechtert.
Verschlüsselte Dateien werden grün Angezeigt.

Bei eigenständigen Computern ist es sehr wichtig, den Schlüssel zu sichern.
In Active Directory-Umgebungen sollte es einen Datenwiederherstellungs-Agenten (Data Recovery Agent, DRA) geben. Der DRA kann auf jede verschlüsselte Datei zugreiffen!

EFS-Einstellungen können über Gruppenrichtlinien konfiguriert werden.

File Replication Services (FRS)

Distributed File System (DFS)

Erfordert: **AD**

Replikation von Dateien zwischen mehreren Servern
Hinweis: So wenig Replikationsgruppen wie möglich bilden.
DFS-Namespace einrichten, bildet den Stamm der freigegebenen Ordner in Ihrer Organisation.
DFS stellt einen einzigen Namespace zur Verfügung, der es Benutzern erlaubt, eine Verbindung zu jedem freigegebenen Ordner in Ihrer Organisation herzustellen.

Es gibt zwei Pooling Optionen:
- Für Konsistenz optimiert
- Für Skalierbarkeit optimiert

Befehlszeilentool: **dfsutil und dfsdiag**

Freigeben von Ordnern

W2k8-Server Rolle: Dateidienste installieren.

Freigabeprotokolle:
- Windows-Protokoll (Server Message Block, SMB)
- UNIX-Protokoll (Network File System, NFS)

Schattenkopien

Schattenkopien ermöglichen es Datensicherungssoftware, auf Dateien zuzugreifen, die gerade benutzt werden.
Schattenkopien speichern nur Kopie + Änderungen.

Befehlszeilentool: **vssadmin**

Drucker

Drucker erfordern einige der kompliziertesten Verwaltungsaufgaben in einer Organisation. Weil Drucker nahe bei den Benutzern aufgestellt sein müssen, ist es unmöglich, sie zu zentralisieren. Benutzen Sie Gruppenrichtlinien in einer AD-Umgebung um die Drucker den Benutzern zur Verfügung zu stellen.

Rolle: Druckdienst installieren
Bietet eine leistungsfähige Benutzeroberfläche für die Verwaltung.

Rollendienste:
- Druckserver
- LPD-Dienst
- Internetdrucken (Erfordert IIS)

Standardisierung
- Stellen Sie zwei oder mehr identische Drucker an jedem Standort bereit und konfigurieren Sie diese Drucker als Druckerpool.
- Installieren Sie alle erforderlichen Druckertreiber für die Client-Systeme
- Beschränken Sie sich auf so wenige Druckermodelle wie möglich.
- Verbinden Sie die Drucker direkt mit dem Kabelnetzwerk und nicht mit Servern.

- Richten Sie Benachrichtigungen ein.
- Richten Sie Druckerprioritäten ein.
- Richten Sie Gruppenrichtlinien ein um die Drucker den Benutzern zur verfügung zu stellen
- Schulen Sie die Benutzer

Druckerpool konfigurieren

Ein Druckerpool besteht aus zwei oder mehr identischen Druckern, auf denen Benutzer ihre Dokumente ausdrucken können, als wäre es ein einziger Drucker.
Drucker in einem Druckerpool müssen denselben Druckertreiber verwenden.

Internetdrucken

Rollendienst: Internetdrucken
Fehler! Linkreferenz ungültig.

Migrieren von Drucker

Benutzen sie die Export/Import-Funktion um einen Drucker von einem Server auf den anderen zu portieren.

Befehlszeilentool: **%SystemRott%\System32\spool\tools\printbrm –b –f printers.printerexport**

Verwalten von Druckern mit Skript

PrnMngr.vbs	Drucker hinzufügen und entfernen
PrnCnfg.vbs	Drucker konfigurieren
PrnDrvr.vbs	Druckertreiber hinzufügen/auflisten etc.
PrnJobs.vbs	Druckaufträge verwalten
PrnPort.vbs	Druckeranschlüsse verwalten
PrnQctl.vbs	Testseite drucken
PubPrn.vbs	Drucker im AD-Veröffentlichen

cscript %SystemRott%\System32\Printing_Admin_Scripts\de-DE\prncfg.vbs -?

IIS - Internet-Information-Server

Standard Benutzerkonto: **IUSR_*Computername***

Lokales Dienstkonto

Das lokale Dienstkonto ist ein integriertes Konto, das dieselben Zugriffsrechte für Ressourcen und Objekte besitzt wie die Mitglieder der Gruppe Benutzer. Durch diesen beschränkten Zugriff wird das System bei Gefährdung einzelner Dienste oder Prozesse geschützt. Dienste, die unter dem lokalen Dienstkonto ausgeführt werden, greifen als NULL-Sitzung ohne Anmeldeinformationen auf Netzwerkressourcen zu. Beachten Sie, dass das lokale Dienstkonto nicht für den SQL Server-Agentdienst oder den SQL Server-Agentdienst unterstützt wird. Der Name des Kontos lautet "**NT AUTHORITY\Local Service account**".

Netzwerkdienstkonto

Das Netzwerkdienstkonto ist ein integriertes Konto, das mehr Zugriffsrechte für Ressourcen und Objekte besitzt als die Mitglieder der Gruppe Benutzer. Dienste, die unter dem Konto Netzwerkdienste ausgeführt werden, können mithilfe der Anmeldeinformationen des Computerkontos auf Netzwerkressourcen zugreifen. Der Name des Kontos lautet "**NT AUTHORITY\NetworkService**".

Lokales Systemkonto

Das lokale Systemkonto ist ein integriertes Konto mit sehr hohen Privilegien. Es hat umfangreiche Privilegien auf dem lokalen System und repräsentiert im Netzwerk den Computer. Der Name des Kontos lautet "**NT AUTHORITY\System**".

Servermodule:
WWW-Server
Gopher-Server
FTP-Server

Internet Server Paket (z.B. Netscape Commerce Server)

CGI 1.1. Installation: Siehe **"Konfigurieren von CGI-Anwendungen"** http://10.63.220.20/iishelp/
Suchen am besten unter Index.

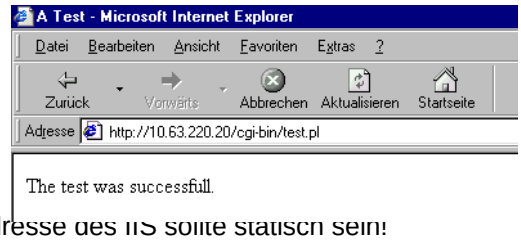
Virtuelles Verzeichnis anlegen: cgi-bin Physisches Verzeichnis \...\Scripte

Perl-Code:

```
#!(usr/local/bin/perl
use CGI;
$query = new CGI;
print $query->header;
print "<html><head><title>A Test</title></head>\n";
print "<body>The test was successfull.</body></html>";
```

Test: Aufrufen mittels http://localgost/cgi-bin/test.pl

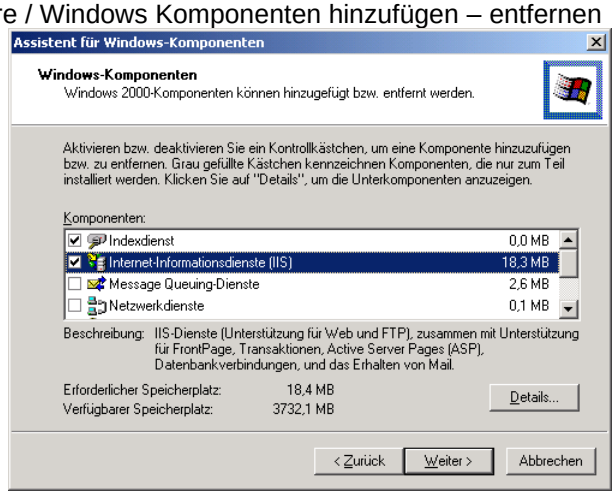
Resultat:



IIS installieren

Empfehlung: Die IP-Adresse des IIS sollte statisch sein!
CD bereithalten

Systemsteuerung / Software / Windows Komponenten hinzufügen – entfernen

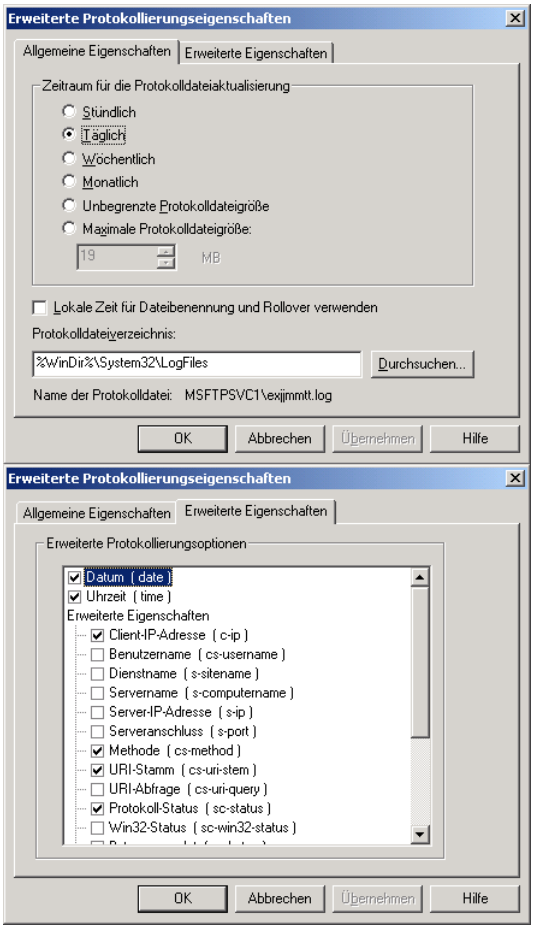


Systemsteuerung / Verwaltung / Internetdienste – Manager

Siehe auch: NT 4.0 Option Pack

FTP-Konfigurieren
Neu / Virtuelles Verzeichnis

FTP-Logfile:
Das FTP Logfile befindet sich standard auf c:\winnt32\system32\logfiles\MSFTPSVC1\exjjmmtt.log



16:10:25 10.41.55.23 [9]USER anonymous 331
16:10:25 10.41.55.23 [9]PASS x.x@swissonline.ch 230
16:13:18 10.41.55.23 [9]created pspbrwse.jbf 226

Web-Site Konfigurieren
Einstellungen

IIS Verwalten

Zustände:

- Wird ausgeführt
- Angehalten
- Beendet

MS Office SharePoint

c:\>**stsadm**

Config DB	Wird bei der Installation erstellt.
Content DB	Für die Zentraladministration

Shared Services

Dokumentenmanagement

ASP.NET im IIS registrieren.
C:\Windows\Microsoft.NET\Framework\v2.0.xxxxx>aspnet_regiis.exe -i

BizTalk Server 2006

Eine Middleware Lösung ähnlich MQ-Series. Über verschiedenste Adaptoren lassen sich diverse Systeme anschliessen.
BizTalk 2006 benutzt XLANG oder WF um die Abläufe zu implementieren.

Internet Secutity & Acceleration Server 2006

Bietet Filtermöglichkeiten auf Anwendungsebene.

Abkürzungen

ACE	Access Control Entry
ACL	Access Control List
AD CS	Active Directory-Zertifikatdienst
AD DS	Active Directory-Datenspeicher (ntds.dit)
AD FS	Active Directory-Verbunddienst
AD LDS	Active Directory Lightweight Directory Services
AD RMS	Active Directory-Rechteverwaltungsdienst
ADI	Active Directory-Integrierte Zone
DACL	Discretionary Access Control List
DC	Domain Controller
DN	Distinguished Name
FQDN	Fully Qualified Domain Name
GC	Global Catalog
GUID	Global Unique Identifier Sind mit Seriennummern für Active Directory-Objekte vergleichbar, haben aber keine bestimmte Bedeutung.
IDA	Identity and Access
MMC	Microsoft Management Console
RODC	Read-Only Domain Controller
RSAT	Remoteserver-Verwaltungstools
SACL	Sytstem Access Control List
SSO	Single Sign On
UNC	Universal Naming Convention

Abbildungsverzeichnis

PowerShell 10
Beispiel einer Gesamtstrukturstammdomäne 13
Gesamtstruktur mit einer einzigen Struktur 13
Gesamtstruktur mit mehreren Strukturen 14
Betriebsmaster Gesamtstruktur 17
Betriebsmaster Schema 18
Betriebsmaster Domäne 18
Gruppen 39
Objekte schützen 39
Vertrauensstellung 47
Policy Names 75
Windows Security Health Validator 76

Index

.

.adm 42
.adml 42
.admlx 42
.clg 49
.inf 45
.msi 44
.msp 45
.mst 44

3

3389 38, 73

A

Acctinfo.dll 28
ACE 84
ACL 84
AD CS 33, 62, 84
AD DS 84
AD FS 34, 36, 84
AD LDS 32, 84
AD RMS 34, 84
AD RMS-Client 34
ADAM 32
ADI 84
ADMT 14
adprep 48
AES 20
AH 72
AIA 34
AIK 49
ALTools.exe 28
Anwendungsverzeichnispartitionen 8, 48
auditpol.exe 46

B

bcedit 50
boot.wim 51
Bridgeheadserver 27

C

CA 34
Cmdlets 10
CN 10, 38
Computerkonfiguration 43
CSE 41, 43, 44

D

DACL 84
DAS 57, 58
DC 84
dcdiag.exe 27
DDNS 70
default.bcd 50
DFS-R 44
DHCP 51
Dienstticket 48
displayName 38
DN 84
DNS 25, 51, 65, 68, 70, 71
dnscmd.exe 71
DRA 26, 44
DRM 35
DS-RPC 26

E

ESP 72

F

Failover-Cluster 60
FC59
Footprinting 70
FQDN 84
FRS 22, 44
FSMO 17

G

GC 14, 24, 84
GNZ 8, 71
GPMC 41
gpmc.exe 42
GPO 41, 42, 44
gpresult.exe 43
GPSI 41, 45
gpupdate 9, 43
Gruppenrichtlinienaktualisierung 43
Gruppenrichtlinienobjekt 41
Gruppenrichtlinienobjekte 41
Gruppenrichtlinienverwaltung 41
Gruppenrichtlinienvorlagen 42
GUID 19, 84

H

Hashcodes 47
Hauptsuchdienst 20
Hintergrundaktualisierung 44
HTTPS 33
Hypervisor-Technologie 55

I

IDA 84
IFM 29
IIFP 32
IIS_IUSRS 34

IKE 72
inetOrgPerson 39
install.wim 49, 51
Installationsabbild 51
ipconfig 66
IPv6 67, 68
IPV6 71
iSCSI 59
ISM-SMTP 27
ISTG 27, 28

K

KCC 25, 26, 44
Kerberos 19
KMS 53

L

ldp.exe 29
LSA-Schlüssel 40
LSASS 14
LUN 58
LZX 49

M

MIIS 32
MILM 32
MMC 84
MOSS 32
ms-DS-MachlneAccountQuota 40
mstsc 38
Multimasterreplikation 32
MUP 44

N

Namenskontext 24
NAS 58
NAT 72
NC 24
NDES 34
NetBIOS 65, 70, 71
NetBIOS-Namen 14
NETLOGON 40
Netzwerkdienst 37
NLA 38
NLB 60
ntds.dit 24, 29, 84
ntdsutil 20
ntdsutil.exe 29
NTLM 46

O

OCSP 34
Online-Responder 34
OWA 33

P

PAS 24
Passthrough-Authentifizierung 47
PDC 20
Phantomobjekt 19
PKI 33
PNRP 71
Polling 26
PowerShell 9, 10
PRP 48
PSO 46
PXE 50, 55
PXE-Server 50

Q

Quorumkonfiguration 60

R

RDN 38
RDP 38
redircmp.exe 40
redirusr.exe 39
Remotedesktop 38
Remoteverwaltung 43
repadmin.exe 27
Replikationstopologie 26
Richtlinie 41
Richtlinieneinstellungen 41
Richtlinienergebnissatz 43
RODC 24, 46, 47, 84
RoundRobin 70
Round-Robin 59, 70
RPC-Server 40
RPCSS 44
RSAT 84
RsOP 9, 43
RSoP 43

S

S/MIME 34
SA 72
SACL 46, 84
SAM 40
sAMAccountName 10, 38
SAN 58, 59
SAN-Fabric 58
SCCM 52
SCEP 34
Schattengruppe 47
Schema 12
schmmgmt.dll 17
secedit.exe 45
Sicherheitsfilter 41
Sicherheitsgruppen 39
Sicherheitsvorlage 45
Sicherheitsvorlagen 9
Sicherungsmedien 29
SID 19, 39, 40

sIDHistory 14
Single Sign On 36
slmgr 52
Smartcards 34
Softwareinstallation 41
Softwareverteilungspunkt 45
Split-Brain Syndrom 70
SRV 23
SSL 33
SSO 36, 84
Standortobjekte 23
Startabbild 51
Systemstatusdaten 30
SYSVOL 16, 22, 44

T

TAPI 25
Task-Manager 30
taskmgrk.exe 30
Teilattributsatz 24
Terminaldienste 38
TFTP-Server 50
Token 17
Tombestonecontainer 29
Tombstonecontainer 29

U

UGMC 24, 25
UNC 84
Unternehmenszertifizierungsstellen 34
UPN 38
userPrinzipalName 38
UTC 20

V

VAMT 52
VDS 58
Verbindungsobjekte 25, 26
Verteilergruppen 39
vertrauende Domäne 47
vertraute Domäne 47
VMRC 55, 57
Volumes 29
Volumeschattenkopie-Dienst 28
VSMT 57
VSS 28

W

W2k8-Server 42
WAIK 30
wbadmin.exe 29, 30
WDS 50
wdsutil 51
Whole-Brain 70
Win32Time 20
WMI-Filter 41, 42
WPAD 70
WQL 42
WSRM 30, 31
WVista 42

X

Xpress 49
XrML 35

Z

Zeitstempel 19