70-680 Konfiguration von Windows 7

Autor	Simon Gattner
Autor Website	http://gattner.name/simon
Dokument Name	70-680.doc
Dokument Titel	Konfigurieren von Windows 7
Dokument URL	http://gattner.name/simon/public/microsoft/Windows%207/70-680.doc http://gattner.name/simon/public/microsoft/Windows%207/70-680.pdf http://gattner.name/simon/public/microsoft/Windows%207/70-680.html
Dokument Datum	2010-11-17
Dokument	*Namen, Eigennamen* $Befehle, ~Dateinamen

Installation von Windows 7

Hardwarevoraussetzungen und Funktionsumfang für Windows 7

Windows 7 Starter* und *Home Basic

- 1GHz
- Min. 512 MB RAM / max. 4GB (x86) bzw. 8GB (x64)
- 20GB (x64) / 16GB (x86) HDD / 15GB SSD
- GC 32MB Speicher, *DirectX 9*
- Keine *Domain*

Windows 7 Home Premium*, *Professional*, *Ultimate* und *Enterprise

- 1GHz
- Min. 1GB RAM / max. 4GB (x86) bzw. 16GB (x64)
- 40GB HDD / 15GB SSD
- GC 128MB Speicher, *DirectX 9, WDDM-Treiber (Windows Display Driver Model), Pixel Shader* 2.0-Hardware, min. 32Bit/px
- *Home Premium* unterstützt keine *Domain*
- *Professional* unterstützt *Domain, EFS, Remotedesktophost*
- *Ultimate* / *Enterprise* unterstützt, *Domain, EFS, Remotedesktophost, AppLocker, DirectAccess, BitLocker, BranchCache*, starten von *VHD*
- *Enterprise* entspricht *Ultimate* wobei *Enterprise* als Volumenlizenz für Unternehmen gedacht ist

Upgrade / Migration auf Windows 7

- Via ***Windows Anytime Upgrade*** von *Windows Vista Business SP2* (Architektur muss übereinstimmen)
- Via Migration von *Windows XP*
- Via Migration von *Windows XP / Vista* oder *7* mit ***USMT*** *(User State Migration Tool)* `$scanstate.exe` bzw. `$loadstate.exe` welches im ***WAIK*** *(Windows Automated Installation Kit)* enthalten ist
- Via Migration von *Windows XP / Vista* oder *7* mit ***Windows-EasyTransfer***
- Sowohl ***Windows-EasyTransfer*** als auch ***USMT*** kann *Benutzerprofile*, *Dokumente* sowie *Applikation*seinstellungen migrieren
- ***Side-by-Side-Migration*** (Übertragung der Benutzerprofildaten von einem alten auf einen neuen Computer)
- ***Wipe-and-Load-Migration*** (Übertragung der Benutzerprofildaten von einer alten Installation auf eine Neu-Installation auf dem gleichen PC)
- In der *Systemsteuerung* kann man via *Systemstart* das *Standartbetriebssystem* festlegen oder man nutzt `$bcdedit.exe`

Konfiguration von Systemabbildern

Windows AIK-Tools (Windows Automated Installation Kit)

Tool	Beschreibung
*Windows **SIM** (Windows System Image Manager)*	Öffnet Windows Abbilder, erstellt Antwortdateien und verwaltet Breitstellungsfreigaben und Konfigurationssätze
ImageX	Dient zum Aufzeichnen, Erstellen, Bearbeiten und Anwenden von Windows-Abbildern
DISM	Wendet Updates, Treiber, Language Packs und Windows-Funktionen auf ein Windows-Abbild an. *DISM* steht in allen Installationen von Windows 7 zur Verfügung
***Windows PE**-Tools*	Das *Windows AIK* enthält mehrere Tools, die dazu dienen, *Windows PE*-Umgebungen aufzubauen und zu konfigurieren
***USMT** (User State Migration Tool)*	Zum Migrieren von Benutzerdaten aus einer älteren Windows-Version auf Windows 7. *USMT* wird als Teil des *Windows AIK* im Verzeichnis `%ProgramFiles%\Windows AIK\Tools\USMT` installiert
Oscdimg	Erstellt ISO-Abbilder

Abbild erstellen für eine LTI bzw. ZTI

1. **SIM** `~autounattended.xml` erstellen
2. ***Referenzinstallation* erstellen** mit `~autounattended.xml`
3. `$Sysprep /oobe /generalize` um die *Referenzinstallation* zu generalisieren
4. ***Windows PE*** vorbereiten via `$Oscdimg`
5. via *Windows PE* und `$ImageX` (`~wimscript.ini`) ein **WIM-Abbild** von der *Referenzinstallation* zu **erstellen**
6. via ***DISM*** das WIM-Abbild bearbeiten und vervollständigen
7. das **WIM**-Abbild auf einem zugänglichen **Datenträger ablegen** um es auf das kopieren durch W*indows PE* vorzubereiten bzw. *WDS* oder *MDT* nutzen.
8. via *Windows PE* Zielrechner Formatieren und Partitionieren mit `$diskpart`
9. via *Windows PE* das Image auf dem Zielrechner aufspielen mit `$ImageX`
10. ***BCDboot** (Boot Configuration Data)* um die Startumgebungsdateien in die Systempartition zu kopieren.

Sysprep
`$Sysprep /audit` startet den Computer im *Überwachungsmodus*. Es laufen die Konfigurationsdurchläufe *auditSystem* und *auditUser.*

`$Sysprep /generaliz` bereitet die *Referenzinstallation* der Abbilder für die Aufzeichnung durch `$ImageX` vor, indem es verschiedene *Computer-* und *Benutzereinstellungen* (z.B. die *SID*) beseitigt und *Protokolldateien* entfernt.

`$Sysprep /oobe` startet den Computer mit der Windows-Willkommensseite neu. Es läuft der Konfigurationsdurchlauf *oobeSystem*.

Konfigurationsdurchlauf	**Beschreibung**
windowsPE	Setzt *Windows PE* Optionen und grundsätzliche Windows-Setupoptionen. *Partitionen*, *Pruduct Key*, *Windows PE Treiber*
offlineServicing	Installiert *Updates* für *das Windows-Abbild, Softwarefixes, Language Packs, Abbild-Treiber*
specialize	Setzt *Netzwerkeinstellungen*, *internationale Einstellungen, Domaininformationen*
generalize	Entfernt *systemspezifische Informationen, hardwarespezifische Einstellungen, SID*
auditSystem	Verarbeitet Einstellungen bei unbeaufsichtigten Setups vor start des *Überwachungsmodus*
auditUser	Verarbeitet Einstellungen bei unbeaufsichtigten Setups im *Überwachungsmodus*
oobeSystem	Verarbeitet Einstellungen bevor die *Windows-Willkommensseite* startet

WIM-Formate (Windows Imaging) koennen mit `$ImageX` erstellt und engewendet werden.
Im Gegensatz zu *ISO-Formaten* enthalten sie ein dateibasiertes Datenträgerformat, dass einen ganzen Satz Dateien und die *Dateisystemmetadaten* enthält.
ISO-Formate sind Sektorbasiert.
WIM-Abbilder sind hardwareunabhängig und können auf *Volumen* oder einer *Partition* bereitgestellt werden.
Die *Low-Level-Datenträgerstrukturen* für *WIM* muss mit einem Tool wie `$diskpart` bereitgestellt werden.

MDT (Microsoft Deployment Toolkit) stellt *Betriebssysteme* und *Anwendungen* bereit, bietet *Treiberverwaltung* und ist als *Distributionsserver* einsetzbar.
MDT kann mit der *LTI (Lite Touch Installation)* und *ZTI (Zero Touch Installation)* arbeiten. Bei *ZTI* benötigt *MDT* allerdings *SCCM* und den *Microsoft SQL-Server*.
MDT setz voraus das Windows AIK installiert ist.
MDT *Deployment Workbench* hilft beim verwalten von verschiedenen Betriebssystem-Abbildern und deren Bereitstellung die geeignet sind zur *LTI* bzw. *ZTI*.
Deployment Workbench kann *Bereitstellungsfreigaben*, *Betriebsystem-Abbilder*, *Gerätetreiber* und *Tasksequenzen* verwalten und anlegen; *Anwendungen*, *Updates* oder *Language Packs* hinzufügen, anlegen und verwalten.

WDS (Windows Deployment Service) stellt eine über *PXE* gestartete *Windows PE-Version* zu Verfügung. *WIM*-Abbildaufzeichnungen auf einem *WDS*-Server ähnelt den Einsatz von `$ImageX` und `$Sysprep`.
WDS ist eine Serverrolle und benötig eine AD DS-Domäne, DNS-Server, DHCP-Server und ein NTFS-Volumen.
WDS ist deutlich schlanker als *MDT*. *WDS*-Abbilder dienen dazu Systemdateien auf Computern bereitzustellen. Es gibt vier verschiedene Abbildtypen:

- ***Installationsabbilder*** *(install images)* sind *Betriebsystemabbild* die auf dem Clients installiert werden
- ***Startabbilder*** *(boot images)* sind *Windows PE-Abbilder* von denen aus der Client gestartet wird
- ***Aufzeichnungsabbilder*** *(capture images*) sind bestimmte *Startabbilder* die genutzt werden um ein Installationsabbild aufzuzeichnen
- **Suchabbilder** (discover images) sind *Startabbilder* die genutzt werden um Clients die nicht *PXE*fähig zu starten

ZTI setzt *MDT 2010* und das *Windows AIK* sowie *SCCM 2007* und einen *MS SQL-Server* voraus in einer *PXE*-Umgebung.
LTI setzt *MDT 2010* und *WDS* voraus.

DISM kann *WIM*s bearbeiten und verwalten:
$mkdir *Volumen:\dism\image*
$dism /mount-wim /wimfile:*Volumen:\to\image\file.wim*
/index:1 /mountdir:*Volumen:\dism\image*
$dism /get-mountedwiminfo
$mkdir *Volumen:\dism\workdir*
$dism /image:*Volume:\dism\image*
/scratchdir:*Volume\:dism\workdir*
$dism /commit-wim /mountdir:*Volume:\dism\image*

(Mit $**imagex** ist es auch möglich *WIM*-Files zu mounten via $imagex /mountrw *Volume:\to\image\file.wim* 1 *Volume:\imagex\image*)

***WIM*-Eigenschaften:**
$dism /get-mounedwiminfo
$dism /get-wiminfo /wimfile:*Volume:\path\to\wim\file.wim*
$imagex /info Volume*:\path\to\wim\file.wim*

***WIM*-Recovery and Cleanup:**
$dism /cleanup-wim (entfernt beschädigte Dateien)
$dism /remount-wim (ermittelt verwaiste Abbilder und remounted sie)
$dism /cleanup-image (/RevertPendingActions) (Probiert eine Systemwiederherstellung)

***WIM*-Informationen:**
$dism /image:Volume:\path\to\online\image [/get-CurrentEdition | /get-targetedition (Zeigt eine Liste der Windowseditionen an auf die aktuallisiert werden kann)| /get-driverinfo | /get-drivers | /get-intl (Internationale Einstellungen und Sprachen) | /get-apps | /get-appsinfo | /get-apppatches | /get-apppatchinfo | /get-packages | /get-packagesinfo | /get-features | /get-featureinfo]

WIM-MSI* und *WIM-MSP:
$dism /image:Volume:\path\to\online\image [/get-apps | /get-apppatches | /get-appsinfo | /get-apppatchinfo]
(Es gibt keinen Schalter /add-apps um *Anwendungen* zu installieren. Dafür eignet sich der *New Application Wizard* aus *MDT*)
***WIM-Packages* (*CAB* und *MSU*) und Features:**
$dism /image:Volume:\path\to\online\image [/get-packageinfo | /add-package | /remove-package | /get-features | /get-featureinfo | /enable-feature | /disable-feature]
$dism /image:Volume:\path\to\online\image /add-package /packagepath:*Volume:\path\to\package\file.cab*
$dism /image:Volume:\path\to\online\image /enable-feature /featurename:Chess
$dism /commit-wim /mountdir:Volume:\to\online\wim (Um die Veränderungen anzuwenden)

***WIM*-Driver:**
$dism /image:Volume:\path\to\online\image [/get-driver | /get-driverinfo | /add-driver | /remove-driver]

$dism /image:Volume:\path\to\online\image /add-driver /driver:Volume:\path\to\driver /recurse

```
$dism /image:Volume:\path\to\online\image /add-
driver:Volume:\path\to\driver\file.inf
```

***WIM*-Einstellungen:**

```
$dism /image:Volume:\path\to\online\image [ /get-intl | /set-
uilang | /set-syslocal | /set-userlocal | /set-timezone |
/distribution ]
```

***WIM*-Windows-Einstellungen:**

```
$dism /image:Volume:\path\to\online\image [ /get-
currentedition | /get-targeteditions | /set-edition | /set-
productkey ]
$dism /online /set-edition:Ultimate /productkey:12345-47382-
38290-37362-12034
```

***WIM-Windows PE*:**

```
$dism /image:Volume:\path\to\online\image [ /get-pesettings
| /get-profiling | /get-scratchspace | /get-targetpath … ]
```

***WIM-Unattend (SIM)*:**

```
$dism /image:Volume:\path\to\online\image [ /apply-
unattend:Volume:\path\to\unattend.xml
```

VHD (Virtual Hard Disk)

- *VHD*s sind virtuelle Festplatten die in einer einzigen Datei enthalten sind. *VHD*-Dateien werden von *Hyper-V, Virtuel Server* und *Virtual PC* für virtuelle *HD*s benutzt.
- *VHD*s sind bootfähig unter *Windows 7 Enterprise* und *Ultimate* lassen sie sich in den `bootmgr` eintragen mit `$bcdedit`.
- *VHDs* können mit *Windows-Bereitstellungsdienste (WDS – Windows Deployment Service)* online verfügbar gemacht, verwaltet und erstellt werden.
- *VHDs* können mit dem ***Offline Virtual Machine Servicing Tool*** plus einem *Solution Accelerator* wie *SCVMM (* installiert von einem *Windows-Server* aus geupdatet (*Windows-Updates*) werden.
- *Solution Accelerator* sind Tool-Sammlungen wie MDS, AIK oder SCVMM

VHDs lassen sich via $**diskpart** oder in der *Datenträgerverwaltung* erstellen.

```
$DISKPART> create vdisk file=Volume:\path\to\vdisk\file.vhd
maximum=20000
$DISKPART> select vdisk file=Volume:\path\to\vdisk\file.vhd
$DISKPART> attach vdisk
$DISKPART> create partition primary
$DISKPART> assign letter=Volumeletter
$DISKPART> format quick label=Description
```

VHDs lasse sich via $**bcdedit** und $**bcdboot** bootfähig machen

```
$bcdedit /copy {current} /d "Description"
$bcdedit /set GUID device
vhd="[Volume:]\path\to\vdisk\file.vhd"
$bcdedit /set GUID osdevice
vhd="[Volume:]\path\to\vdisk\file.vhd"
$bcdedit /set GUID detecthal on
$bcdedit /v
```

WIM-Abbild und Bootdateien in die **VHD** kopieren

```
$imagex /apply Volume:\path\to\image\file.wim #n1
volume:\path\to\add\the\image
$bcdboot Volume:\current\bootfiles Volume:\of\added\image
```

Geräte-Manager (Treiber und Hardware)

PnP-Geräte können von *Nicht-Administratoren* installiert werden wenn der *Treiber* eine gültige *digitale Signatur* hat die mit *Zertifikaten* im Speicher *Vertrauenswürdige Herausgeber* verknüpft sind.
PnP-Geräte müssen von einem *Administrator* installiert werden wenn der *Treiber* sich nicht im *Treiberspeicher* befindet, *unsigniert* ist oder die *Signatur* als nicht vertrauenswürdig eingestuft wird.

Unsignierte Treiber können vom *Administrator* mit einem *Zertifikat* aus einer internen *Zertifizierungsstelle* signiert werden das *Standartbenutzer* das *Gerät* installieren können.

```
$mmc devmgmt.msc
```

Systemsteurung -> Hardware und Sound -> Geräte und Drucker -> ***Geräte-Manager***
Startmenü -> Computer -> (recht- klick)*Verwaltung ->* Konsolenstruktur *-> Computerverwaltung*

.inf Treiberinstallationsdateien
.sys Treiberdateien

Geräte-Manager gestartet auf einem *Remotecomputer* lassen sich kein *Treiber installieren*, *deinstallieren* oder die Vorversion *wiederherzustellen*.

Geräte-Manager *->* Gerät *Eigenschaften -> Allgemein -> Gerätestatus* (Zeigt den Status des Gerätes an und bei Problem Fehlermeldungen oder Fehlercodes)

Geräte-Manager *-> Legacyhardware hinzufügen* installiert *Treibersoftware* für *Nicht-PnP-Geräte*.

Geräteinstallationseinstellungen bestimmt das Verhalten mit von *Windows Update* bereitgestellter *Treibersoftware*.
Default Einstellung ist *Ja, automatisch aufühen (empfohlen)*.
Um *Treibersoftware* vorher zu testen sollte die Option *Nein, zu installierende Software selbst auswählen -> Nie Treibersoftware von Windows Update installieren* aktiviert sein.

```
$mmc gpedit.msc -> Internetkommunikationseinstellungen ->
Suche nach Gerätetreibern auf Windows Update deaktivieren
```

Staging eines *Gerätetreibers* beschreibt den Prozess des genehmigen eines *Gerätes* vom *Administrator* wenn kein *Gerätetreiber* im *Treiberspeicher* vorliegt.
Staging durchsucht den *Treiberspeicher*, prüft *Benutzerrechte* und die *Signatur* des *Treibers*. Nur *Administratoren* können das installieren eines *unsignierten Geräte-Treibers* zulassen.

Ressourcenkonflikte treten bei *PnP-Geräten* eher selten auf. *Konflikte* entstehen meist bei der Überschneidung von *Ressourcen* (*Gerät -> Eigenschaften* -> Reiter *Ressourcen*), z.B. wenn ein *Nicht-PnP-Gerät Ressourcen* des *Motherboards* beansprucht.
Konflikte lassen sich temporär durch das deaktivieren eines der am *Konflikt* beteidigten *Geräte* beseitigen. *Konflikte* lassen sich langfristig meist durch das *aktualisieren* (falls ein neuer *Treiber* vorhanden ist) oder das *deinstallieren* und neu *installieren* der *Hardware* lösen.
`$mmc devmgmt.msc -> (Ansicht -> Ausgeblendete Geräte einblenden) Nicht-PnP-Geräte`

`$msinfo32 -> Systemübersicht -> Hardwareressourcen -> Konflikte/Gemeinsame Nutzung`
`$msinfo32 -> Systemübersicht -> Komponenten -> Problemgeräte`

`$dxdiag` (Grafik- und Sound- und Eingabe-Geräte Informationen)

`$sigverif` (Durchsucht den Computer nach unsignierte Treibern)

`$driverquery /si` (Listet alle Gerätetreiber auf)

Treiberüberprüfungs-Manager
`$verifier`
`$verifier /volatile` (Überprüfung eines Treibers ohne den Computer neu zu starten)
`$verifier /faults` (Testet Treiber und simuliert Stresstests bei den z.B. die Ressourcen knapp werden)

`$pnputil -a Volume:\path\treiber\*.inf` (Stellt einen Treiber im Treiberspeicher bereit)
`$pnputil -e` (Listet Treiber auf)

$regedit -> HKEY_LOCAL_MACHINE -> Software -> Microsoft -> Windows -> CurrentVersion -> DevicePath: %System-Root%\inf; Volume:\other\driver\path;Volume:\more\other\driver\path

Geräteintallationsrichtlinien (lokale Gruppenrichtlinien, GPO)
`$mmc gpedit.msc -> Computerkonfiguration -> Administrator Vorlagen -> System -> Geräteinstallation -> Einschränkungen bei der Geräteinstallation`

`$mmc gpedit.msc -> Computerkonfiguration -> Administrator Vorlagen -> System -> Treiberinstallation -> Treiber für diese Geräte-Setupklassen ohne Administratorrechte zulassen`

Geräte-Setupklassen oder auch *Geräteklassen* (***GUID***) finden sich im *Geräte-Manager* im Reiter *Details* unter *Geräteklassen-GUID* des gewälten *Gerätes*.

Verwalten von Datenträgern

Ein *Volumen* kann aus mehreren *Partitionen* zusammengefügt werden.
Ein *Volumen* ist auch ein *RAID (Redundant Array of Independent Disk)* 1 Verband aus hd0 und hd1 mit jeweils einer *Partition* auf hd0 und einer *Partition* auf hd1.
Ein *Volumen* ist virtuell angelegt.
Eine *Partition* ist physikalisch angelegt.

*Volumen -> Eigenschaften -> Bereinigen -> **Datenträgerbereinigung*** (Dialog)
*Volumen -> Eigenschaften -> Bereinigen -> **Datenträgerbereinigung** -> **Systemdateien Bereinigen** -> Systemwiederherstellung und Schattenkopien* (kann nur von Administratoren ausgeführt werden)

`$defrag /c /h /u` (Defragmentiert alle Volumen und Wechseldatenträger bei denen es sinnvoll ist / geht nicht unter Windows XP)
*Volumen -> Eigenschaften -> Tools -> **Jetzt defragmentieren*** (Zeitplan / Analysieren / Defragmentieren)

Defragmentieren von *Festplatten*, *USB-Flashsticks* und *VHDs* erhöht die Leistung.
Nur *NTFS-Volumen* können defragmentiert werden.
Volumen mit einem *Fragmentierungsgrad* höher als 10% sollten defragmentiert werden. Es kann nur ein *Zeitplan* für die *Defragmentierung* angelegt werden.

*Volumen -> Eigenschaften -> Tools -> **Fehlerüberprüfung** -> Jetzt prüfen* (Optionen der Datenträgerprüfung: *Dateisystemfehler automatisch korrigieren*; *Fehlerhafte Sektoren suchen/wiederherstellen*)

Datenträgerrichtlinien (lokale Gruppenrichtlinien, GPO)
Lese- oder Schreibezugriff auf *Wechseldatenträger / CD und DVD / Diskettenlaufwerk* / *Bandlaufwerke oder benutzerdefinierte Klassen (via eingabe der GUID)* verweigern
`$mmc compmgmt.msc` *Datenträgerspeicher -> Datenträgerverwaltung*

MBR-Datenträger können maximal 2GB groß sein.
GBT-Datenträger können mehr als vier *Partitionen* enthalten.
MBR-Datenträger können *zu GPT-Datenträger* oder *dynamischen Datenträgern* konvertiert werden und andersherum solang sie kein *Volumen* enthalten.
`$DISKPART >convert (mbr|gbt|basic|dynamic)`

Dynamische-Datenträger benutzen einen reservierten Bereich auf dem Datenträger um *LDM-Datenbanken (Logical Disk Manager*) zu speichern. *LDMs* enthalten *Volumen*-Informationen die auf jedem *Dynamischen-Datenträger* repliziert werden.
Dynamische-Datenträger sind zuverlässiger.
Dynamische-Datenträger sollten nicht einzeln verschoben werde.
Dynamische-Datenträger müssen importiert werden auf fremden Geräten.
Dynamische-Datenträger sind nur schwer in *Basis-Datenträger* (*MBR/GBT*) zurück zu konvertieren da die *LDM* Datenträgerübergreifend abgelegt sind.
`$DISKPART >online` (reaktiviert offline oder fehlende dyn. Datenträger)
`$DISKPART >create volume simple [size=<n>] [disk=<n>]`
`$DISKPART >shrink querymax`
`$DISKPART >extend [size=<n>] [disk=<n>]`
`$mountvol` (Volumen bereitstellen)

Übergreifende Volumen (*Stripsetvolumes*) sind zusammengesetzt aus mehreren Teilen von *Dynamischen-Datenträgern*.
Stripsetvolumes (*RAID-0*) verwenden mehrere physische Festplatten um ein *Volumen* zu bilden (min. 2 Datenträger). Garantiert schneller Datenzugriff. *Stripesetvolumen* müssen auf *Dynamischen Datenträgern* erstellt werden.
`$DISKPART >create volume stripe [size=<n>] [disk=<n>[,<n>[…]]`

Gespiegelte Volumes (*RAID-1*) verwenden mehrere physische Festplatten um ein *Volumen* zu bilden (min. 2 Datenträger). Garantiert Ausfallsicherheit.
`$DISKPART >select disk`
`$DISKPART >add disk=<n>`

Stripsetvolumes mit Parity (*RAID-5*) verwenden mehrere physiche Festplatten um eine *Volumen* zu bilden (min. 3 Datenträger). Garantiert schneller Datenzugriff und Ausfallsicherheit.
`$DISKPART >create volume raid [size=<n>] [disk=<n>[,<n>[…]]`

Bereitstellungspunkte (*Windows Hardlinks*) stellen Ordnerinhalte eines Ordners oder Volumen an anderen Punkten bereit.
`$fsutil hardlink` *`Volume:\UrsprungsOrdner Volume:\Ziel\Ordner`*

Verwaltung von Anwendungen

Anwendungskompartibilität

`Programm` (Recht Maustaste) -> *Behandeln von Kompatibilitätsproblemen*
Programmbehandlung für Programmkompatibilität versucht automatisch Probleme zu beheben.
`Programm` (Rechte Maustaste) -> *Eigenschaften -> Kompatibilität*
Vordefinierte Kompatibilitätsmodi und Optionen die ältere *Betriebssysteme* nachahmen, *Farbraum*, *Visuelle Designs*, *Desktopgestaltung*, *DPI-Werte* deaktivieren oder *Bildschirmauflösung* verkleinern bzw. das Programm *als Administrator* oder *anderen Benutzer ausführen*.

ACT (Application Compatibility Toolkit)

Tool	Funktion
Application Compatibility Manager	Sammelt und analysiert Kompatibilitätsdaten. Erfasste Daten werden in einer *SQL Server-Datenbank* gespeichert (es wird also ein *MS SQL-Server* benötigt). Erstellt *DCP*s (*Data Collection Packages*) für einzelne Clients. Eignet sich für eine große Anzahl von Clients.
Compatibility Administrator	Eignet sich für eine große Anzahl von Anwendungskompatibilitätsproblemen. Hat bereits eine Datenbank mit bekannten *Kompatibilitätsfixes*. Kann *Kompatibilitätsfixes* erstellen. Ein *Kompatibilitätsmodus* ist eine Sammlung von *Kompatibilitätsfixes*.
Internet Explorer Compatibility Test Tool	Testet Webanwendungen auf ihr kompatibilität mit *Internet Explorer 8* (Standart *IE* bei *Windows 7*).
Setup Analysis Tool	Überwacht Aktivitäten von Installationsprogrammen. Kann Kompatibilitätsprobleme bei der Installation von: *Kernelmodustreibern*, *16-Bit-Komponenten* und *GINA-DLL*s (*Graphical Identification and Authentication Dynamic-Link Libraries*) und *Windows-Ressourcenschutz* entdecken.
Standard User Analyzer	Erkennt Kompatibilitätsprobleme die durch die *Benutzerkontensteuerung* entstehen. Liefert Daten zu: *APIs, Registrierschlüsseln, .ini-Dateien, Token, Berechtigungen, Namespaces* und *Prozessen*.

Lokale Gruppenrichtlinien Andwendungskompatibilitätsdiagnose
Computerkonfiguration -> Administrative Vorlagen -> System -> Problembehandlung und Diagnose -> Andwendungskompatibilitätsdiagnose

`$sdbinst` (Installation von *Skim's* (*Anwendungskompatibilitätsfixes*))

Windows XP Mode für Windows 7 stellt ein *Windows XP Umgebung* mit *Microsoft Virtual PC* unter *Windows 7 Professional*, *Enterprise* und *Ultimate* zu Verfügung.
In der *Windows XP* Umgebung installierte Anwendungen werden automatisch im *Startmenü* von *Windows 7* angezeigt.
Eine so gestartete Anwendung sieht aus wie eine *Windows 7* Anwendung.
Windows XP Mode setzt einen Prozessor mit *AMD-V* oder *Intel VT* voraus (muss oft im *Bios* aktiviert werden) und min. *256MB RAM* je *XP-Mode-Client*.
Windows XP Mode bietet eine x86-Version *Windows XP Professional SP3* Version.
Windows XP Mode unterstützt keine x64-Anwendungen.
Windows XP Mode Windows XP Version muss ebenfalls gepatched werden.
Windows XP Mode wird heruntergefahren wenn ein Programm direkt *im XP Modus* aus dem *Startmenü* gestartet wird.

Lokale Gruppenrichtlinien zur Softwareeinschränkung

Computerkonfiguration -> Richtlinien -> Windows-Einstellungen -> Sicherheitseinstellungen -> ***Richtlinien für Softwareeinschränkungen***

Richtlinien für Softwareeinschränkungen lassen sich auf *Windows XP, Vista* und *Windows 7-Editionen* anwenden die kein *AppLocker* vorhalten.
Richtlinien für Softwareeinschränkungen legen eine *Standartregel* fest die entweder alle Anwendungen blockiert oder alle Anwendungen zulässt.
Richtlinien für Softwareeinschränkungen werden in folgender hierarchischen Reihenfolge angewendet:

i. ***Hashregel*** (Digitaler *Fingerabdruck* / *Checksum*)
ii. ***Zertifikatregel*** (*Herausgeberzertifikate*)
iii. ***Pfadregel*** (Datei- oder Ordner-Angabe)
iv. ***Netzwerkzonenregel*** (Unterscheiden *Installer* nach dem Download-Ort. Sie gelten nur für *.msi*-Dateien die mit dem *IE* heruntergeladen wurden.)

Richtlinien für Softwareeinschränkungen haben folgende *Sicherheitsstufen*:

- *Nicht erlaubt*
- *Standartbenutzer* (im Gegensatz zu *Administratoren*)
- *Nicht eingeschränkt*

Richtlinien für Softwareeinschränkungen *-> Erzwingen* (legt fest ob auch *DLLs* mit einbezogen werden)
Richtlinien für Softwareeinschränkungen -> Designierte Dateitypen (legt fest welche *Dateitypen* als *Ausführbare-Datei* eingestuft werden)

AppLocker

AppLocker-Anwendungsrichtlinien stehen auf *Windows 7 Editionen Enterprise* und *Ultimate* zur Verfügung und sind vergleichbar mit *Richtlinien* für *Softwareeinschränkungen*.
AppLocker-Anwendungsrichtlinien lassen sich jedoch auf *Benutzer*- und *Gruppen-Konten* anwenden und können auch für zukünftige Versionen eines Produkts gelten.
AppLocker-Anwendungsrichtlinien sind darauf angewiesen das der *Dienst Anwendungsidentitäten* läuft.
AppLocker-Blockierungsregeln haben Vorrang vor *AppLocker-Zulassungsregeln*.
AppLocker-Regeln werden auch *Anwendungssteuerungsrichtlinien* genannt.
AppLocker-Regeln können via *Regeln automatisch generieren* mit Hilfe eines Assistenten erstellt werden bei dem man den *Pfad* der Datei oder des Verzeichnisses und Typ der Regel angibt.
AppLocker-Überwachung protokolliert nur das Zutreffen von Regeln und setzt sie nicht durch. Wenn *AppLocker* Regeln nur überwacht konfigurieren sich die entsprechenden Regeln im Knoten der *Local GPO -> AppLocker* entsprechend.
AppLocker hat Vorrang vor den *Richtlinien für Softwareeinschränkungen.*

`$mmc gpedit.msc` *-> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Anwendungsteuerungsrichtlinien ->* ***AppLocker***

Typ	Eigenschaft
Standartregeln	Automatisch erstellte Regeln die notwendig sind weil *AppLocker* über eine *Blockierungsregel* (*fallback block rule*) verfügt die alle Anwendungen blockiert. *Standartregeln* lassen deshalb die meisten *Anwendungen* zu. Die Benutzer-Gruppe Jeder ist Standarteintellung.
Blockierungsregeln	Blockieren oder lassen Anwendungen zu. *Blockierungsregeln* haben Vorrang vor *Standartregeln*. Mit *Blockierungsregeln* kann die Ausführung von *Anwendungen*, die durch *Standartregeln* zugelassen sind, verhindert werden. Die *Benutzer-Gruppe Jeder* ist Standarteinstellung.
Ausführbare Regeln	Regeln für ausführbare Dateien (.*exe*, .*bat*, .*vbs* etc.). *Standartregeln* sind *Pfadregeln* die Anwendungen aus dem Ordnern *Programme* und *Windows* ermöglichen oder *Administratoren* erlauben überall Anwendungen auszuführen.
Windows Installer-Regeln	Gelten für Dateien mit Namenserweiterung .*msi* und .*msp*. Kann die Installation von Software regeln. Die Standartregeln erlauben der *Benutzer-Gruppe Jeder* aller digital signierter Windows Installer-Dateien und aller Windows Installer Dateien aus dem Verzeichnis `%SystemDrive %Windows\Installer` und *Administratoren* das ausführen aller .*msi* und .*msp*-Dateien.
Scriptregeln	Gelten für Datein mit Namenserweiterung .*ps1*, .*bat*, .*cmd*, .*vbs* und .*js*. Für Scripts die nur selten geändert werden sollten *Hashregeln* erstellt werden und *Pfadregel* für Ordner in denen die Scripte gespeichert sind. Die *Standartregeln* lassen das ausführen aller Scripte zu, die in den Ordnern *Programme* und *Windows* gespeichert sind. Administratoren können von überall Scripte ausführen.
DLL-Regeln	Gelten für Dateien mit der Namenserweiterung .*dll* und .*ocx*. *DLL-Regeln* werden bei der Aktivierung von *AppLocker* nicht automatisch aktiviert. *DLL-Regeln* bieten ein Höchstmaß an Sicherheit auf kosten der Leistung.
Herausgeberregeln	Überprüfung von Dateien anhand des *Codesignaturzertifikats*. Details der digitalen Signatur werden aus einer Referenzanwendung gelesen. *Herausgeberregeln* gelten auch für zukünftige Versionen einer Datei, im Gegensatz zu *Hashregeln*. Es lassen sich auch bestimmte Datei-Versionen einschränken.
Hashregeln	Überprüfung von Dateien anhand eins *digitalen Fingerabdrucks* (*Hashwert* / *Checksum*). *Hashwerte* können automatisch erstellt werden. Es ist auch möglich *Hashwerte* für einen Ordner zu erstellen.
Pfadregeln	Überprüfung von Dateien oder Ordnern anhand des *Pfades*.
Ausnahmeregeln	Bestimmte Anwendungen lassen sich von allgemein formulierten Regeln ausnehmen.

Netzwerkeinstellungen

CIDR-Notation (Classless Inter Domain Routing) schreibt man eine *Subnetmask* 255.255.255.0 -> **/24.** 24 weil binär 11111111.11111111.11111111.00000000 24x1 gefolgt von 8x0.
Das Netz 192.168.0.0 mit der *Subnetzmask* 255.255.255.0 kann auch als 192.168.0.0/24 angegeben werden.
Die ***CIDR**-Subnetmask* /25 in binärer *Punktnotation*: 11111111.11111111.11111111.100 00000; in der dezimaler *Punktnotation* 255.255.255.128 ist.
Die private *B-Classen Netz* 192.168.0.0 mit der *CIDR-Subnetmask* /25 hat den *Netzwerkmaske* 192.168.0.128, die *Broadcast-Adresse* 192.168.0.255 und kann den *IP-Bereich* von 192.168.0.129-192.168.0.254 abdecken.

***DHCP** (Dynamic Host Control Protocoll)* weist *Hosts* dynamisch *IP-Adressen*, *Standardgateways* und *DNS-Server* zu falls so eingestellt.

***DNS** (Domain Name System)* löst sowohl *lokale Hostnamen* als auch *FQDN (Fully Qualified Domain Name)* nach *IPs* auf und *IPs* auf *Hostnames* als auch *FQDN*.
Stellt ebenfalls *DNS-Surffixes* zu Verfuegung.
DNS-Surffixes sind *Hosts* hinter dem @ bei *E-Mail-Adressen*.

***APIPA**/ZCN (Zero Configuration Networking, auch Automatic Private IP Addressing, kurz APIPA, oder Auto-IP)* konfiguriert ein *internes privates Netzwerk* ohne *DHCP*.
Wenn ein Netzwerk keine Verbindung zu anderen Netzen hat kann man *APIPA* benutzen um die Computer miteinander kommunizieren zu lassen.
APIPA konfiguriert *IPv4*-Einstellungen eines Computers mit einer *IPv4-Adresse* im bereich von 169.254.0.1 bis 169.255.254 mit der Subnetzmask 255.255.0.0.
APIPA konfiguriert kein *Standardgateway*, weil *APIPA* konfigurierte *Netzwerke* keine *IPv4-Pakete* in andere *Netzwerke* sendet oder empfängt.

***NAT** (Network Address Translation)* konfiguriert ein *privates Netzwerk* über eine einzelne *öffentliche IPv4-Adresse* um zugriff auf das *Internet* zu erhalten. *NAT routet* die *öffentliche, WAN (Wide Area Network) IPv4-Adresse* mit der *private, LAN (Local Area Network) IPv4-Adresse*.

***IANA** (Internet Assigned Numbers Authority)* vergibt und verwaltet *öffentliche IPv4-Adressen* ueber verschiedene Unterorganisationen.

***RIPE** (Réseaux IP Europèes)* ist seit 1989 die europäische Unterorgnaisation der *IANA* zum verwalten und vergeben von *IPv4-Adressen*.

***LAN** (Local Area Network)*, bzw. *private Netzwerk-Adress-Blöcke* die die *IANA* zugeteilt hat:

- 10.0.0.0/8 (10.0.0.1 bis 10.255.255.254)
- 172.16.0.0/12 (172.16.0.1 bis 172.31.255.254)
- 192.168.0.0/16 (192.168.0.1 bis 192.168.255.254)

Außerdem wird auch der *APIPA-Bereich* 169.254.0.0/16 (169.254.0.1 bis 169.254.255.254) als *privater Adress-Block* behandelt da seine Adressen nie im *Internet* auftauchen. *APIPA-Adressen* sind aber wiederum keine *LAN-Adressen*.
***SOHO**-Netze (Small Office Home Office)* sind *LANs*.

ICS *(Internet Connection Sharing)* und ***WAP*** *(Wireless Access Point)* sind verschiedene Arten mit denen ein Computer ins Internet verbunden werden kann. Beim *ICS* oder *WAP* teilt ein so konfigurierter Computer seine Internetverbindung mit anderen.

WLAN (*Wireless Local Area Network*) Authentifizierungstypen:

- ***Gemeinsam verwendet*** (ein vorinstallierter Schlüssel) sollte nur verwendet werden wenn keine der folgenden Authentifizierungstypen möglich ist.
- ***WPA-Personal*** (*Wi-Fi Protected Access* mit *PSK*) für kleine Netzwerke die in keiner Domäne liegen. Der Aufwand für Computerzertifikate zu hoch ist und *WPA2* nicht möglich ist.
- ***WPA2-Personal*** (mit PSK) für kleine Netzwerke die in keiner Domäne liegen und moderne Hardware mit AES bieten.
- ***WPA-Enterprise*** und ***WPA2-Enterprise*** gleichen den *Personal*-Versionen bis auf das Zertifikate auf den Client-Computern abgelegt werden müssen.
- ***802.1X*** (*Portbasierte Authentifizierung meist mit einem RADIUS-Server*) ist die Sicherste Lösung.

WLAN Technologien

- ***802.11b*** 11Mbit/sec. und hohe Signalreichweite
- ***802.11a/g*** 54Mbit/sec. geringe / sehr hohe Signalreichweite
- ***802.11n*** > 54Mbit/sec.

Netzwerk- und Freigabencenter -> Verbindung zu einem Drahtlosennetz herstellen
Netzwerk- und Freigabencenter -> Drahtlosnetzwerk verwalten

```
$netsh wlan
$netsh wlan show interfaces
$netsh wlan connect name=<Profilname> ssid=<Netzwerk-SSID>
[interface=<Schnittstellenname>]
$netsh wlan disconnect interface=*
$netsh wlan disconnect interface=”Drahtlosnetzwerkverbindung”
```

IPv6

IPv6 ist der Nachfolger von *IPv4*. Im Gegensatz zu *IPv4* hat *IPv6* einen *Adressraum* von 2^128 Adressen (*IPv4* hat einen *Adressraum* von 2^32) was für jeden Quadratmeter Erdoberfläche 6,5 x 2^23 oder 54.525.952 Adressen ausmacht. *IPv6*-Adressen werden also nicht so schnell ausgehn.
128Bit lange *IPv6*-Adressen werden in *Blöcke* von *16Bit* unterteilt. Jeder *Block* wird in eine 4-Stellige Hexadezimalzahl konvertiert.
Doppelpunkte dienen als Trennzeichen. Diese Darstellung wird *als Doppelpunkt-Hexadezimal-Format* bezeichnet.
Globale Unicast-IPv6-Adressen entsprechen öffentlichen *Unicastadressen* in *IPv4*.

Bsp. Eine *Unicast-IPv6-Adresse*:
21cd:0053:0000:0000:03ad:003f:0000:8d62
21cd:53:0:0:3ad:3f:0:8d62 (führende Nullen in einem Block können ausgelassen werden)
21cd:53::3ad:3f:0:8d62 (Blöcke die den Wert 0 haben können mit :: einmal zusammengefasst werden)

Präfixe von *IPv6*-Adressen werden wie bei *IPv4* mit *Schrägstrichnotationen* angegeben.
Zum Bsp. Ist 21cd:53::/64 das *Subnetz* in dem die Adresse 21cd:53::3ad:3f:0:8d62 liegt. Die forderen 64Bit sind das *Netzwerkpräfix*. *Subnetpräfixe* (die *Subnetz-ID*) wird einer einzelnen *Verbindung* (*link*) zugewiesen. Demselben *link* können mehrere *Subnetz-IDs* zugewiesen sein, was man auch als *Multinetting* bezeichnet.

ND (*Neighbor Discovery*) löst *IPv6*-Adressen in *MAC*-Adressen auf. Der 64Bit lange Hostabschnitt einer globalen *IPv6*-Unicastadresse leitet sich aus der *MAC*-Adresse ab.

Host werden mit Hilfe von ***DNS*** aufgelöst, außer bei *verbindungslokalen* Adressen. Wertepaare aus Computername und *IPv6*-Adresse in einem *AAAA-DNS-Ressourceneintrag* gespeichert, dem Gegenstück zum *A*- oder *Hosteintrag* bei *IPv4*. *Reverse-DNS-Lookups*, die den Computernamen zu einer *IPv6*-Adresse liefern, werden in einem *PTR-DNS-Ressourceneintrag* implementiert, der über *die IPv6-Reverse-Lookupzone ipv6.arpa* führt. Die *Reverse-Lookupzone in-addr.arpa* ist das *IPv4* Gegenstück.

In *Peer-to-Peer*-Umgebungen ohne *DNS* kann ***PNRP*** (*Peer Name Resolution Protocol*) eingesetzt werden. *PNRP* kann *Peernamen* mit dem Computer oder Diensten verknüpfen und diese Daten geschützt (Kryptografie) oder ungeschützt veröffentlicht werden.

***IPv6*-Adresstypen** (*RFC 2373*):

- ***Unicast*** identifiziert eine einzelne *Schnittstelle* innerhalb des Bereichs des *Unicastadresstyps*. Pakete werden an eine einzige *Schnittstelle* geliefert. Es ist erlaubt mehrere *Schnittstellen* dieselbe Adresse zuzuweisen, sofern die *Schnittstellen* für die *IPv6*-Implementierung auf dem *Host* wie eine einzige *Schnittstelle* aussehen (ermöglicht *Lastverteilungssysteme*).
  IPv6-Unicastadressen
  i. `2n{3}:` ***Globale*** *Unicastadressen* sind das *IPv6*-Gegenstück zu öffentlichen *IPv4*-Adressen. Sie sind global routingfähig, zusammenfassbar (*aggregatable global unicast address*), zusammenfassbare globale *Unicastadressen* sind im gesamten *IPv6*-Internet eindeutig. (Bereiche in dem eine *IP*-Adresse eindeutig ist, wird als *Gültigkeitsbereich* oder engl. *Scope* bezeichnet.)
  Formatpräfix (*Format Prefix, FP*) sind die drei höchsten Bits die immer `001` sind. Theoretisch beginnen Unicastadressen mit `2` oder `3`, in der Praxis beginnen sie mit `2`.
  Die hinteren 64Bits einer *Unicastadresse* definieren den *Host* und werden entweder von der 48Bit langen *MAC-Hardware-Adresse (Media-Access-Control)* abgeleitet oder der *NIC* zugewiesen.
  Die *Schnittstellenidentität* wird also von der Netzwerkkartenhardware zu Verfügung gestellt. (*RFC 2374*)
  ii. `fe80:` ***Verbindungslokale*** (***link-local***) *IPv6*-Adressen sind das Gegenstück zu *APIPA* konfigurierten *IPv4*-Adressen.
  Der Gültigkeitsbereich ist die lokale Verbindung.
  Sie werden immer automatisch Konfiguriert.
  iii. `fec0:` ***Standartlokale*** (***site-local***) *IPv6*-Adressen sind das Gegenstück zum privaten *Adressraum* in *IPv4*. Private Intranets die keine Verbindung in das *IPv6*-Intranet haben, können *standortlokale* Adressen verwenden, ohne dass ein Konflikt mit zusammenfassbaren globalen *Unicastadressen* entstehen.
  Der *Gültigkeitsbereich* einer *standortlokalen* Adresse ist der Standort.
  Sie können z.B. mit *DHCPv6* zugewiesen werden.
  Hosts verwenden *standortlokale* Adressen wenn *Routerankündigungsnachrichten* empfangen werden die kein *Adresspräfix* enthalten.
  Teredo-Tunnel verwenden solche Adressen.
  iv. *Speziell IPv6*-Adressen sind unspezifizierte Adresse und *Loopbackadressen*.
  `0:0:0:0:0:0:0:0` oder `::` ***unspezifizierte Adresse*** steht für das Fehlen einer Adresse. Sie ist das Gegenstück zur *unspezifizierten IPv4-Adresse* `0.0.0.0`.
  Sie wird normalerweise als Quelladresse eingetragen um zu überprüfen ob eine vorläufige Adresse eindeutig ist.
  Sie wird niemals einer *Schnittstelle* zugewiesen oder als Zieladresse verwendet.
  `0:0:0:0:0:0:0:1` oder `::1` ***Loopbackadressen*** identifizieren eine *Loopbackschnittstelle*.
  Sie ist das Gegenstück zur *IPv4-Loopbackadresse* `127.0.0.1`.

- ***Multicast*** identifiziert mehrere *Schnittstellen*. Pakete die an eine *Multicastadresse* gerichtet sind, werden an mehrere *Schnittstellen* geliefert die mit der Adresse *identifiziert* werden.
  IPv6-Multicastadressen
  i. Mithilfe einer `ff00:` ***IPv6-Multicastadresse*** kann ein *IPv6*-Paket an mehrere Hosts gesendet werden die alle die selbe *Multicastadresse* haben.
     Das *FP* lautet 11111111.
- ***Anycast*** identifiziert mehrere *Schnittstellen*. Pakete die an eine *Anycastadresse* geliefert werden, werden an die nächstgelegene *Schnittstelle* geliefert die durch die *Schnittstelle* identifiziert wird (nächstgelegen bedeutet mit geringster Routingentfernung oder wenigsten *hops*).
  IPv6-Anycastadressen
  i. Eine *Anycastadresse* ist mehreren *Schnittstellen* zugewiesen. Pakete, die an eine *Anycastadresse* gerichtet sind, werden von der *Routinginfrastruktur* an die nächstgelegene dieser *Schnittstellen* weitergeleitet.
     Die *Routinginfrastruktur* muss bekannt sein, welche zugewiesen sind und wie weit sie im bezug auf die *Routingmetrik* entfernt sind.
     Im Moment werden *Anycastadressen* nur als Zieladressen verwendet und sie werden Routern zugewiesen.

IPv6 wurde entwickelt um die Nachteile von *IPv4* zu überwinden. *IPv6* hat folgende **Vorteile gegenüber *IPv4***:

- **Größerer *Adressraum*** (2^128)
  Der *64Bit-Hostabschnitt* (*Schnittstellen-ID*) kann aus der *NIC* generiert werden.
- **Automatische Adresskonfiguration**
  IPv4 wird normalerweise von Hand oder mit *DHCP* konfiguriert. Automatische konfiguration (*APIPA*) ist nur in isolierten Subnetzen möglich. *IPv6* bietet eine einfache automatische Adresskonfiguration die sowohl statusbehaftete als auch statusfreie Adresskonfiguration zulässt.
- **Sicherheit auf Netzwerkebene**
  IPSec (*Internet Protocol Security*) bietet die Möglichkeit Kommunikation über das Internet zu verschlüsseln. *IPv6* macht *IPSec* obligatorisch.
- **Datenauslieferung in Echtzeit**
  IPv4 nutzt *QoS* (*Quality of Service*) um Bandbreite für Echtzeitverkehr zu garantieren. Dies gilt aber nicht wenn *IPv4*-Pakete verschlüsselt sind.
  Im *Feld Flow Label* des *IPv6*-Headers ist eine NutzdatenIdentifizierung eingebaut, so dass der *QoS*-Betrieb auch mit Verschlüsselungfunktioniert.
- **Größe der Routingtabelle**
  Routingtabellen von Backboneroutern sind deutlich kleiner dank Routenzusammenfassung.
- **Headergröße und Erweiterungsheader**
  IPv4- und *IPv6*-Header sind nicht kompatibel.
  Hosts und Router müssen eine *IPv4*- und *IPv6*-Implementierung enthalten um beide Header-Formate zu erkennen und zu verarbeiten.
  IPv6-Header sind möglichst kompakt aufgebaut. Alle nicht unbedingt benötigten (optionalen) *Felder* wurden in den Erweiterungs-Header verschoben.
- **Kein Broadkastverkehr**
  IPv4 nutzt *ARP*-Broadcasts um die *MAC*-Adresse der *NIC* aufzulösen. *IPv6*-Nachbarermittlungsprotokoll (*Neighbor Discovery, ND*) arbeitet mit einer Abfolge von *ICMPv6*-Nachrichten. *ND* ersetzt *ARP*-Broadcasts, *ICMPv4*-Routersuche und *ICMPv4*-Umleitungsnachrichten durch effiziente *Multicast*- und *Unicast-ND*-Nachrichten.

IPv4-zu-IPv6-Kompatibilität

0:0:0:0:0:0:0:a.b.c.d oder ::a.b.c.d ***IPv4*-kompatible Adressen** von *Dual-Stack-Knoten* die über *IPv4*-Infrastruktur mit *IPv6* kommunizieren.

0:0:0:0:0:ffff:a.b.c.d oder ::ffff:a.b.c.d ***IPv4*-zugeordnete Adressen** werden benutzt um reine IPv4-Knoten einem IPv6-Knoten bekannt zu machen.

2002:ab:cd::/16 **6to4-Adressen** kann benutzt werden um *IPv6*-Pakete über ein *IPv4*-Netzwerk zu transportieren ohne das Tunnel konfiguriert werden müssen. Ermöglicht *IPv4*-Clients den Zugang in das *IPv6*-Internet und ist als Übergangslösung geplant.

2001::/32 **Toredo-Adressen** (*RFC 4380*) enthalten ein *32Bit-Teredo-Präfix*. Auf das *Präfix* folgt die 32Bit lange *IPv4*-Adresse des *Teredo*-Servers der die Adresse mitkonfiguriert.
Die nächsten 16Bit sind für *Teredoflags* reserviert.
Die nächsten 16Bit speichern die *UDP*-Port-Nummern, die den gesamten *Teredo*-Verkehr abwickelt.
Die letzten 32Bit speichern die externe *IPv4*-Adresse die den gesamten *Teredo*-Verkehr abwickelt.

… :5efe: … *IPv6* kann **ISATAP-Adressen** (*Intra-Site Automatic Tunneling Adressing Protocol*) nutzen um die Kommunikationen zwischen zwei Knoten über ein *IPv4*-Intranet herzustellen.
Die ersten 64Bits beginnen mit *verbindungslokalen*, *standortlokalen*, *globalen* oder *6to4-globalen Unicastpräfixen*.
Die nächsten 32Bits enthalten die *ISATAP*-Kennung 0:5efe.
Die letzten 32Bits enthalten die *IPv4*-Adresse in *Hex*- oder *Punkt-Dezimal-Notation*.
ISATAP-Adressen sind für öffentliche oder private *IPv4*-Adressen.

IPv6-zu-IPv4-Kompatibilität

```
$netsh interface ipv6 6to4
$netsh interface ipv6 isatap
$netsh interface ipv6 add v6v4tunnel
$netsh interface ipv6 add v6v4tunnel “Remote” 10.0.0.11
192.168.123.116
```

IPv6-Konfiguration und Konnektivität (Netzwerkeinstellungen)

*Systemsteuerung -> Netzwerk- und Freigabencenter -> **Internetoptionen***

```
$inetcpl.cpl

$netsh interface ipv6 show address
$netsh interface ipv6 show address level=verbose (listet die
Standort-IDs auf)

$netsh interface ipv6 set address name="LAN-Verbindung"
fec0::ffee:2
$netsh omterface ipv6 add dnsserver name= "LAN-Verbindung"
fec0::ffee:0:0:ff
$netsh interface ipv6 add route ::/0 name="LAN-Verbindung"
fec0::ffee:0:0:1
$netsh interface ipv6 set interface name= "LAN-Verbindung"
forwarding=enabled


$netsh interface ipv6 show neighbors
$netsh interface ipv6 delete neighbors
$netsh interface ipv6 show destinationcache
$netsh interface ipv6 delete destinationcache

$netsh interface ipv6 show route
$route print
$netstat –r
```

IPv4-Konfiguration (Netzwerkeinstellungen)

*Systemsteuerung -> Netzwerk- und Freigabencenter -> **Internetoptionen***

```
$inetcpl.cpl

$netsh interface ip[v4] set address name="LAN-Verbindung"
static 10.0.0.2 255.255.255.0 10.0.0.1
$netsh interface ip[v4] set dnsservers name="LAN-Verbindung"
static 10.0.0.1

$netsh interface ip[v4]set address name="LAN-Verbindung"
source=dhcp
$netsh interface ip[v4] set dnsserver name="LAN-Verbindung"
source=dhcp
```

Netzwerkdiagnose

```
$ping
$ping6
$tracert
$pathping
$nslookup
$netstat
$route
$ipconfig

$ipconfig /all
$ipconfig /release
$ipconfig /renew
$ipconfig /flushdns
$runas /user:administrator ipconfig /registerdns
```

Netzwerk- und Freigabencenter -> Adaptereinstellungen ändern (rechte Maustaste auf gewünschte Schnittstelle) -> *Diagnose*
Netzwerk- und Freigabencenter -> Rotes X (zwischen den *Computer*-, Internet- oder *Netzwerk-Symbol*)
Netzwerk- und Freigabencenter -> Problem beheben
Internet Explorer -> Diagnose von Verbindungsproblemen

1. ***Kabel* und *Hardware*** prüfen (Sind *Computer*, *Modem*, *ICS*, *WAP* an. Stecken alle *Kabel* (LAN-Kabel und Netzkabel). Sind alle notwendigen *Geräte* (*NIC*) aktiviert und laufen fehlerfrei.)
2. Stimmen die ***Netzwerkeigenschaften*** (Korrekte *IP-, DHCP-, DNS-, Gateway-Einstellungen*)
3. ***Firewall*** und Softwareeinstellungen (Temporär die Standarteinstellungen der *Windows-Firewall* wiederherstellen oder die *WFAS (Windows Firewall with Advanced Security)* für kurze Zeit deaktivieren. Evtl. andere Software prüfen und deaktivieren. *Hardwarefirewall, IPsec*.)
4. ***Treiber*** (Sind die *Netzwerktreiber* aktuell. Wurden sie vor kurzem aktualisiert. Funktioniert der Netzwerkzugriff mit dem vorherigen Treiber.)

Netzwerkstatistik

```
$netstat –e –s | more
$netstat –s –p tcp | more
$netsh interface ip show tcpstats
$netsh interface ip show udpstats
```

Windows-Firewall

```
$netsh firewall
$netsh firewall show config
$netsh advfirewall reset
```

Netzwerkstandartkategorien (***Network Location Awareness***, ***NLA***) legen mit dem passenden *Netzwerkprofil* den richtigen Firwallregelsätze fest.
Es gibt Netzwerkprofile für zwei Netzwerktypen:

1. *Domänennetzwerke, Heimnetzwerke, Arbeitsplatznetwerke (privat)*
2. *öffentliche Netzwerke*

Beim verbinden mit einem neuen Netzwerk bietet Windows 7 ein Dialogfeld für die Wahl zwischen ***Heimnetzwerk, Arbeitsplatznetzwerk*** und ***Öffentliches Netzwerk***.
Das *Netzwerkprofil* für *Domänennetzwerke* wird von *NLA* automatisch zugewiesen beim anmelden bei der *Domäne*.
Für verschiedene Netzwerkkarten können verschiedene *Netzwerkprofile* gelten (was bei Windows Vista nicht mögllich war).

Windows-Firewall Netzwerkprofile können nur mit Administratorrechten geändert werden.
Windows-Firewall kann nur *Regeln* auf Basis von *Programmen* und *Windows 7-Funktionen* erstellen. Im Gegensatz zu *WFAS* die auf Basis von *Diensten* oder *Ports Regeln* erstellen kann.

Systemsteuerung -> Windows-Firewall (Anwendungsbezogene Regeln im Gegensatz zum komplexeren *Paketfilter* der *WFAS*)

Systemsteuerung -> System und Sicherheit -> ***Windows-Firewall*** (*Standart wiederherstellen*)

WFAS (Windows Firewall with Advanced Security) IPsec

```
$wf
$mmc wf.msc

$netsh advfirewall firewall add rule name=“ICMPv4“
protocol=icmpv4:any,any dir=in action=allow
$netsh advfirewall firewall add rule name=”ICMPv6”
protocol=icmpv6:any,any dir=in action=allow

$netsh advfirewall firewall add rule name=”HTTPD”
profile=domain protocol=TCP dir=in localport=80 action=allow

$netsh advfirewall firewall add rule name=”SSHD” dir=in
programm=”C:\Windwos\System32\sshd.exe”

$netsh advfirewall firewall add rule name=”FTP” dir=out
program=”C:\Windows\System32\ftp.exe” action=block

$netsh advfirewall (export|import)
```

Systemsteuerung -> Windows-Firewall -> Erweiterte Einstellungen

***WFAS* komplexe Regeln:**

- *Regeln* für *eingehende* und *ausgehende Verbindungen*
- *Regeln* auf Basis von *Protokolltypen* und *Portadressen*
- *Regeln* auf Basis der *Adresse* des Absenders oder Empfängers
- *Regeln* die nur *Authentifizierten Datenverkehr* zulassen
- *Verbindungssicherheitsregeln* (authentifizierter und verschlüsselter Datenverkehr / ähnelt *IPsec-Richlinien*, ist aber nicht unter *Windows XP* verfügbar)

***WFAS* Regeltypen:**

- *Programm Regeln*
- *Port Regeln*
- *Vordefinierte Regeln*
- *Benutzerdefinierte Regeln* (Dienste oder Programm + Port)

***WFAS* Regeloptionen:**

Die *WFAS* Standarteinstellung setzt voraus, dass die Verbindung authentifiziert und integritätsgeschützt, aber unverschlüsselt ist.

- *Verbindung zulassen*
- *Verbindung blockieren*
- *Verbindung zulassen, wenn sie sicher ist* (*WFAS* lässt die Regel zu wenn eine der Methoden authentifiziert wird die in den *Verbindungssicherheitsregeln* festgelegt ist)
- *Verschlüsselung der Verbindung erforderlich* (setzt voraus, dass die Verbindung authentifiziert, integritätsgeschützt und verschlüsselt ist)
- *zum Blockieren außer Kraft setzen* (kann Computerkonto oder Computergruppe ausnehmen)

Regel-*Bereiche* legen fest ob eine Regel für gewisse Quell- und Ziel-Adressen gilt.
Regel-*Bereiche* gibt es nur bei *benutzerdefinierten Regeln*.
Regel-*Erweitert* legt fest für welche *Gerätetypen* (*NAT*) die Regel gilt.

***WFAS Verbindungssicherheitsregeln*-Typen:**

- ***Isolierungsregeln*** können die Kommunikation auf bestimmte Hosts beschränken die mit bestimmten Anmeldeinformationen authentifiziert sind. Mit *Isolierungsregeln* kann z.B. die Kommunikation gesperrt werden mit Hosts die nicht in der *AD DS-Domäne* sind.
- ***Authentifizierungsausnahmen*** konfigurieren Ausnahmen für *Isolierungsregeln.*
- ***Server-zu-Server*** Regeln können Verbindungen zwischen bestimmten Hosts mit bestimmten Adressen schützen.
- ***Tunnel*** ähneln *Server-zu-Server* Regeln, gelten aber für Remoteverbindungen.

IPSec und IPv6-Paketfilter

Konsolen Snap-In *IP-Sicherheitsrichtlinien*
Konsole Snap-In *Windows-Firewall mit erweiterter Sicherheit*

```
$mmc
$mmc wf.msc
```

Remoteverwaltung

Remotedesktop kann sich nur anmelden wenn kein anderer Benutzer am Remoterechner angemeldet ist. Der Computer muss eingeschalten und hochgefahren sein.
Der Remotecomputer kann aus dem Ruhezustand beim Eingang einer *Remotedesktopverbindungsaufforderung* reaktiviert werden wenn *WOL* (*Wake on Lan*) der *NIC* aktiviert ist.
Ist der Remotecomputer gesperrt kann nur der gesperrte Benutzer sich Remote anmelden.
Ist ein anderer Benutzer angemeldet erhält er eine Meldung, dass sich ein anderer Benutzer remote Anmelden möchte. Der Benutzer kann dies immer ablehnen.
Ist eine Remotebenutzer angemeldet und ein lokaler Benutzer möchte sich anmelden gilt das gleiche.
Das Windows Server 2008 *Terminaldienstegatway* ermöglicht das anmelden von Benutzer über *Remotedesktop* auf Hosts aus dem Internet.
Remotedesktopverbindungen lassen auf den *Windows 7 Editionen: Professional, Enterprise* und *Ultimate* verwenden.
Die *Remotedesktop-Client*-Software ist auf allen **Windows 7 Editionen** enthalten.
Wird *Remotedesktop* aktiviert werden automatisch *Windows-Firewall* Regeln aktiviert.
Um *Remotedekstopverbindungen* mit *Windows XP* zu ermöglichen muss die Option *Verbindung von Computern zulassen, auf denen eine beliebige Version von Remotedesktop ausgeführt wird*.
Wird die *Windows-Firewall* auf *Standarteinstellungen* zurückgesetzt, muss der *Remotdesktop* erneut aktiviert werden.
Um *Standartbenutzern Remotedesktopverbindungen* zu ermöglichen müssen diese der Benutzergruppe *Remotedesktopbenutzer* beitreten.
Mitglieder der Benutzergruppe *Administratoren* und *Remotedesktopbenutzer* können *Remotedesktopverbindungen* aufbauen.

Remoteunterstützung unterscheidet sich in sofern von *Remotedesktop*, dass der Remotecomputer-Benutzer eine Verbindung beim Verwaltungscomputer anfordert.
Remoteunterstützung ist ein *Supporttool*, das dem Supportmitarbeiter ermöglicht den Bildschirminhalt des Remotecomputer-Benutzers einzusehn.
Windows-Firewall Regeln werden automatisch aktiviert beim start einer Sitzung.
Nachdem Windows-*Remoteunterstützung* gestartet hat besteht die Wahl zwischen: *Eine Verstrauenswürdige Person um Unterstützung einladen oder Einem Benutzer, von dem Sie eingeladen wurden, Hilfe anbieten*.
Einladungen können via *E-Mail*, *Speichern der Einladung in einer Datei oder Easy Connect-Methode* (nur wenn *PNRP* auf einem lokalen *Windows 2008 Server* aktiviert ist) erzeugt und verschickt werden.
Neben der *Einladung* wird ein *Kennwort* benötigt das getrennt von der Einladung übermittelt werden sollte.

Systemeigenschaften -> Remote

Windows-Remoteverwaltungsdienst ermöglicht das ausführen von Befehlen auf einem Remoterechner via *WinRS* oder der *Windows PowerShell*.

Lokale GPO -> Computerkonfiguration -> Administrative Vorlagen -> Windows-Komponenten -> Windows-Remoteverwaltung

`$WinRM quickconfig` (Startet den *WinRM*-Dienst auf dem Remotecomputer und konfiguriert die *WinRM*-Firewallausnahmen)

Windows-*Remoteshell*

```
$WinRS –r:<Hostname> [-u:<Benutzername>] [-p:<Kennwort>]
[<Befehl>]
$WinRS –r:http://aberdeen.contoso.internal –u:foo net accounts
$WinRS –r:aberdeen arp
$WinRM set winrm/config/client/
@{TrustedHosts=”<Hostname>,<Hostname>…”}
```

Windows *PowerShell*

Windows *PowerShell* >= *v2* eigenet sich zur Remoteverwaltung

```
$Icm <Hostname> {<Befehl>}
$Icm aberdeen {Get-Process}
```

`$Icm New-PSSession` (erstellt eine dauerhafte Sitzung mit dem Remotecomputer)

BranchCache und Ressourcenfreigabe

Heimnetzgruppen vereinfachen das Freigeben von Dateien und Druckern in *SOHO*-Netzwerken.
Heimnetzgruppen können nur in Netzwerken verwendet werde, die das *Netzwerkprofil Heimnetzwerke* (*privat*) haben.
Netzwerkadressen können hierfür auf *Heimnetzwerk* automatisch eingestellt werden.
Heimnetzgruppen können nicht in Domänen eingerichtet werden, man kann einer vorhandenen *Heimnetzgruppe* aber beitreten.
Heimnetzgruppen haben ein Passwort, man muss sich mit ihm authentifizieren wenn man beitreten will.
Heimnetzgruppen können nur von Benutzern mit Administratorrechten aktiviert werden.
Heimnetzgruppen sehen im Netzwerk *Ressourcen* wie *Datei*-, *Drucker*- und *Bibliothekfreigaben* falls die *Netzwerkerkennung* aktiviert ist.
Heimnetzgruppenfreigaben werden separat im *Windows Explorer* dargestellt.

Systemsteurung -> Netzwerk und Internet -> Heimnetzgruppen

Freigegebene Ordner können *Ordner Eigenschaften -> Freigabe* erstellt und verwaltet werden.
Freigegebene Ordner können auch nur für *Heimnetzgruppen* freigegeben werden.
Erweiterte Freigabe erlaubt spezielle Berechtigungen zu setzen.
Freigegebene Ordner Offlineeinstellungen können in den *Eigenschaften -> Freigabe -> Erweiterte Freigabe -> Zwischenspeicher* konfiguriert werden.

```
$net share
$mmc compmgmt.msc -> Freigegebene Ordner
```

Die Konsole *Computerverwaltung -> Freigegebene Ordner* zeigt alle auf dem Computer freigegebenen Ordner an. Freigaben können hinzugefügt, gelöscht, Offlineeinstellungen vorgenommen und Berechtigungen verändert werden.
Die Konsole zeigt ebenfalls an welche Benutzer auf die Ressourcen zugreifen.

```
$net share <Freigabenname>=Volume:\path\to\share
[/grant:<Benutzer> (Read | Change | Full)]
$net share <Freigabenname> [cache:(manuel | documents |
program | branchcache | none)] [user:<n>]
```

Bibliotheken sind virtualisierte Sammlungen von Ordnern. Die Ordner können aus verschiedenen Dateisystemen, Festplatten und Freigaben stammen.
Bibliotheken werden separat im *Windows Explorer* dargestellt.
Bibliotheken können für eine *Heimnetzgruppe* freigegeben werden.

Druckerfreigaben ermöglichen Benutzern, Dokumente an einen Drucker zu senden, der im Netzwerk an einen anderen Computer angeschlossen ist.
Für ältere Windows Versionen können Drucker-Treiber zur Freigabe hinzugefügt werden.
Druckerfreigaben -> Sichheitseinstellungen erlauben folgende Optionen: eigene Dokumente kontrollieren und *Drucken, Diesen Drucker verwalten,* (alle) *Dokumente verwalten*
Systemsteuerung -> Geräte und Drucker

NTFS-Berechtigungen werden vererbt. Hat z.B. die Gruppe *foobar* für den Ordner *Alpha* die Berechtigung *Ändern*, erhält die Gruppe auch standartmäßig die Berechtigung *Ändern* für alle Unterordner und Dateien die in *Alpha* erstellt werden.
Berechtigungsablehnungen haben Vorrang vor ***Berechtigungszulassungen***.
Vererbte Berechtigungen lassen sich ändern *Eigenschaften -> Sicherheit -> Erweitert -> Berechtigungen ändern -> Vererbbare Berechtigungen des übergeordneten Objektes einschließen* entfernen
Ermitteln der ***effektiven Berechtigung*** hilft wenn der Benutzer Mitglieder in mehreren Gruppen ist. Über *Eigenschaften -> Sicherheit -> Erweitert -> Effektive Berechtigungen*
Ordner und Dateien sind ***Objekte***.
Werden *Objekte* in ein anderes *Objekt kopiert*, erbt das *kopierte Objekt* die *Berechtigungen* des *übergeordneten Objekts*.
Werden Dateien in einen anderen Ordner auf dem *gleichen Volumen verschoben*, behalten die Dateien ihre *Berechtigungen*.
Werden Dateien in einen anderen Ordner auf ein *anderes Volumen verschoben*, bekommen die Dateien die *Berechtigungen* des *übergeordneten Objekts* vererbt. Die Dateien verhalten sich hier wie beim kopieren.
`$robocopy` kann Dateien und ihre *NTFS-Berechtigungen* kopieren. `$robocopy` kann auch dazu dienen Dateien und deren *Berechtigungen* auf ein anderes *Volumen* zu *verschieben*.
Werden *Objekte* auf ein *FAT* oder *FAT32 Volumen verschoben* oder *kopiert* gehen alle *NTFS-Berechtigungen* verlohren.
Freigabe- und ***NTFS-Berechtigungen*** gelten beide wenn ein Benutzer auf freigegebene *Ressourcen* zugreift. Es gilt immer die restriktivere *Berechtigung*.
Ist die ***Überwachung*** von Dateien und Ordnern in den *GPOs* aktiviert, lassen sich über *Eigenschaften -> Sicherheit -> Erweitert -> Überwachung* Gruppen zur Überwachung hinzufügen. *Überwachungsereignisse* werden im *Sicherheitsprotokoll* erfasst und können über die *Ereignisanzeige* eingesehn werden.

Eigenschaften -> Sicherheit

`$mmc gpedit.msc` -> *Computerconfiguration -> Windows-Einstellungen -> Lokale Richtlinien -> Sicherheitsoptionen -> Überwachung*
`$mmc gpedit.msc` -> *Computerconfiguration -> Windows-Einstellungen -> Lokale Richtlinien -> Sicherheitseinstellungen -> Erweiterte Überwachungsrichtlinienkonfiguration -> Systemüberwachungsrichtlinien*

`$icacls` *Volume:\Path[\file]* `(/grant | /deny) <Benutzer | Gruppe>(OI)(F | M | RX | R | W)`

- F Full Controll, Vollzugriff
- M Modify, Ändern
- RX, Read, Execute, Lesen, Ausführen
- R Read, Lesen
- W Write, Schreiben

```
$icacls Volume:\Path[\file] /save file.acl /T
$icacls Volume:\Path[\file] /restore file.acl
```

```
$robocopy Volume:\Copy\Path Volume:\Target\Path /copyall /e
```

Ordner- und Dateiberechtigungen *NTFS Standartberechtigungen*

Berechtigung	**Ordner**	**Dateien**
Schreiben	*Schreiben*	*Schreiben, nicht löschen*
Lesen	*Lesen*	
Ordnerinhalt anzeigen	*Ordnerinhalt anzeigen*	
Lesen, Ausführen	*Lesen, Ausführen; Ordnerinhalte anzeigen; Lesen; Schreiben;*	
Ändern	*Ändern; Lesen, Ausführen; Ordnerinhalte anzeigen; Lesen; Schreiben;*	
Vollzugriff	*Vollzugriff* (Berechtigungen ändern)*; Ändern; Lesen, Ausführen; Ordnerinhalte anzeigen; Lesen; Schreiben;*	

Spezielle Berechtigung	**Voll-zugriff**	**Ändern**	**Lesen, Aus-führen**	**Ordner-inhalt an-zeigen**	**Lesen**	**Schreiben**
Ordner durchsuchen / Datei ausführen	X	X	X	X		
Ordner auflisten / Daten lesen	X	X	X	X	X	
Attribute lesen	X	X	X	X	X	
Erweiterte Attribute lesen	X	X	X	X	X	
Dateien erstellen / Dateien schreiben	X	X				X
Ordner erstellen / Daten anhängen	X	X				X
Attribute schreiben	X	X				X
Erweiterte Attribute schreiben	X	X				X
Unterordner und Dateien löschen	X					
Löschen	X	X				
Berechtigungen lesen	X	X	X	X	X	X
Berechtigungen ändern	X					
Besitz übernehmen	X					

EFS (*Encrypting Files System*) ist in *den Editionen Professional, Enterprise und Ultimate* von *Windows 7* verfügbar.

```
$cipher
```

EFS unterscheidet sich in sofern von *BitLocker* das *EFS* Dateien und Ordner auf Dateiebene verschlüsselt nicht auf Volumenebene.
EFS verschlüsselt im Gegensatz zu *BitLocker* nicht nur für bestimmte Computer, Benutzer oder Gruppen sondern Zertifikatabhängig.
EFS verwendet eine Verschlüsselung mit öffentlichen Schlüsseln (*Public Key Encryption*).
Ein Benutzer verfügt über zwei Schlüssel: Einen *Öffentlichen Schlüssel* der im Zertifikatspeicher des Computers aufbewahrt wird und jedermann zugänglich ist.
Benutzer können den *öffentlichen Schlüssel* zum verschlüsseln von Daten benutzen.
Der *Private Schlüssel* wird im privaten *Zertifikatsspeicher* des Benutzers gespeichert und kann nur vom Benutzer verwendet werden.
Mit dem *Privaten Schlüssel* lassen sich Daten entschlüsseln.
Beim ersten verschlüsseln erstellt *Windows 7 EFS-Zertifikat* und einen *Privaten Schlüssel*.

EFS kann nur Dateien verschlüsseln die auf *NTFS-Volumen* gespeichert sind.
EFS verschlüsselte Dateien und Ordner werden mit dem *Windows Explorer* standardmäßig *grün* angezeigt.
EFS kann keine komprimierten Dateien verschlüsseln, diese werden automatisch dekomprimiert.
EFS Dateien werden automatisch entschlüsselt wenn sie auf ein *FAT-Volumen kopiert* oder *verschoben* werden.
EFS ermöglicht Dateien für mehrere Benutzer zu verschlüsseln sofern alle Benutzer ein *EFS-Zertifikat* im *Zertifikatspeicher* des Computers liegen haben.
EFS kann keine Dateien für *Gruppen* verschlüsseln.

EFS-Zertifikate können in einer *AD DS* zentral verwaltet werden.

EFS-verschlüsselte-Dateien können mit Hilfe eines *Wiederherstellugsagenten* wiederhersgestellt werden.
Wiederherstellungsagenten sind *Zertifikate*.
Wiederherstellungsagenten können alle verschlüsselten Dateien eines Computers mit einem *privaten Schlüssel* wiederherstellen die nach dem Einrichten eines *Wiederherstellungsagenten* verschlüsselt wurden.

```
$cipher /r:recoveryagent
```

Lokale GPO -> Computerconfiguration -> Windows-Einstellungen > Sicherheitseinstellungen -> Richtlinien für öffentliche Schlüssel -> Verschlüsselte Dateien

BranchCache beschleunigt den Zugriff auf Dateien durch *Zwischenspeicherung* in einer *AD DS* bei *Remoteverbindungen*.
BranchCache funktioniert ab *Windows Server 2003* (*Gehosteter Cache*).
BranchCache funktioniert mit *Windows 7 Edition Ultimate* und *Enterprise* (*Verteilter Cache*).
BranchCache benötigt spezielle *Windows-Firewall* Regeln je nachdem ob *Gehosteter* oder *Verteilter Cache* aktiviert ist. *Inhaltsabrufe* verwenden *HTTP*; *Verteilte Caches* verwenden *WSD* für die *Peerermittlung*; *Gohostete Caches* verwenden *HTTPS* für *Gehostete Cacheclients*.

```
$netsh branchcache
$netsh branchcache set service mode=(distributed|local|
hostedclient location=<Cachserver>)
```
(konfiguriert auch die Windows-Firewall Einstellung)
```
$netsh branchcache set cachesize
$netsh branchcache set localcache
```

`$mmc service.msc` -> *BrancheCache*

Lokale GPO -> Computerkonfiguration -> Administrative Vorlagen -> Netzwerk -> BranchCache

Gehostete Caches sind zentrale lokale Zwischenspeicher die auf einem Server eingerichtet werden.
Gehostete Caches sollten verwendet werden wenn in beiden Zweigstellen ein *Windows Server 2008-R2-Server* zu Verfügung steht, da bei *verteilten Caches* Teile nicht zu Verfügung stehen wenn die Clients heruntergefahren sind.
Gehostete Caches eignet sich für Organisationen, die nicht über ihr eigens *AD-Zertifikatdiensteinfrastrautkur* verfügen oder nicht die Ressourcen haben um in jeder Zweigstelle einen *Windows Server 2008 R2-Server* aufzubauen.
Gehostete Caches sollte durch *DFS* (*Distributed File System*) ersetzt werden wenn der *Traffic* im *WAN* Performance-Einbusen verursacht.

Verteilte Caches verwenden *Peercaching* um den Zwischenspeicher auf den *Windows 7-Clients* der Zweigstellennetzwerke zu verteilen.
Verteilte Caches sorgen dafür, dass ein Peer einen Teil des Zwischenspeichers aufnimmt aber niemals den Gesammten.
Wenn ein *Windows 7-Client* eine Datei aus dem *WAN* abfragt, speichert er diese in seinem Zwischenspeicher. Falls ein anderer BranchCache-Client die Selbe Datei anfragt, kann er sie direkt vom ersten Client abrufen und speichert diese wiederum in seinem Zwischenspeicher.

Benutzerkontensteurung

UAC (*User Account Control*) oder auch ***Benutzerkontensteuerung*** ist ein Instrument um festzulegen wann *Administratorrechte* nötig sind um einen Vorgang auszuführen.
Für *Standartbenutzer* ist die *UAC* standardmäßig deaktiviert da er nicht mit der *Benutzerkontensteuerung* zutun hat.

Anheben der Rechte (*privilege elevation*) Alle Benutzer auf *Windows 7-Clients* arbeiten mit Rechten des *Standartbenutzers*. Bei einer Aktion, die das *Anheben der Rechte* erfordert, wechselt *Windows 7* in den *Administratorberechtigungsmodus*.

Administrationsberechtigungsmodus fordert auf zur Eingabe von *Anmeldeinformation* oder *Bestätigung*, für das *Anheben der Rechte*.

Sicherer Desktop verhindert, dass die Eingabeaufforderung zum *Anheben der Rechte* manipuliert oder übergangen werden kann. Der *Desktop* wird in der Zeit in der der *Sichere Desktop* aktiv ist eingefroren. *Windows 7* lehnt nach 150sec. das *Anheben der Rechte* automatisch ab wenn keine Eingabe erfolgt.

Systemsteuerung -> Benutzerkonten -> Einstellungen für Benutzerkontensteuerung

- **Immer benachrichtigen** (Sicherer Desktop) informiert bevor Programme Änderungen am Computer oder den *Windows-Einstellungen* vornehmen
- **Nur benachrichtigen, wenn Änderungen am Computer von Programmen vorgenommen werden** (Sicherer Desktop)
- **Nur benachrichtigen, wenn Änderungen am Computer von Programmen vorgenommen werden (Desktop nicht abblenden**) informiert nur über Programme Drittanbieter
- **Nie Benachrichtigen** informiert nicht bei Änderungen. *Standartbenutzer* die das *Anheben der Rechte* für Aktionen benötigen, werden diese automatisch abgelehnt

```
$mmc secpol.msc
$gpupdate /force /wait:0
```

Lokale GPO -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Sicherheitsoptionen

- *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratormodus*
- *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standartbenutzer*
- *Benutzerkontensteuerung: Anwendungsinstallationen erkennen für erhöhte Rechte anfordern*
- *Benutzerkontensteuerung: Nur Dateien heraufstufen, die signiert und überprüft sind*
- *Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen*
- *Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop*

Authentifizierung

Anmeldeinformationsverwaltung speichert Benutzer und Kennwörter zur Anmeldung am System, Netzwerkressourcen, Websites oder *Terminalserver*.
Windows-Tresor speichert diese Anmeldedaten.
Windows-Tresor empfängt von der *Anmeldeinformationsverwaltung* Anmeldeinformationen wie z.B. die des *Internet Explorer*, der *Remotedesktopverbindung* oder des *Windows-Explorer* (Netzwerkressourcen).
Windows-Tresor Daten lassen sich über die *Anmeldeinformationsverwaltung* Importieren und Exportieren.
Windows-Tresor Daten lassen sich über die *Anmeldeinformationsverwaltung* auch schon vor der eigentlichen Verwendung anlegen.

`$runas /user:<Computername>\<Benutzernamen> "Anwendung.exe /Option"`
`$runas /savescrad` bewirt das die Anmeldeinformationen im *Windows-Tresor* gespeichert werden
`$runas /(no)profile` läd (kein) *Benutzerprofil*

Lokale GPO -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Zuweisen von Benutzerrechten

Vordefinierte Benutzergruppen in *Windows 7*:

- ***Administratoren*** haben unbeschränkten zugriff auf den *Windows 7*-Computer
- ***Sicherungs-Operatoren*** können Zugangsbeschränkungen von Dateien und Ordnern außer Kraft setzen, um Daten zu sichern
- ***Kryptografie-Operatoren*** können kryptografische Vorgänge durchführen. (Kommt nur zum Einsatz wenn *Windows 7* im *Common Criteria Mode* konfiguriert ist. Die Gruppe dient dazu Einstellungen in den *IPsec-Richtlinien* vorzunehmen – was *Administratoren* nicht dürfen)
- ***Distributed COM-Benutzer*** können *Distributed COM-Objekte* auf dem Computer bearbeiten
- ***Ereignisprotokollleser*** können die *Ereignisprotokolle* lesen
- ***Netzwerkkonfigurations-Operatoren*** können Adress-Einstellungen für *TCP/IP* ändern
- ***Leistungsprotokollbenutzer*** können Protokolle von *Leistungsindikatoren* in die *Aufgabenplanung* eintragen, *Ablaufsverfolgungsanbieter* aktivieren und *Ereignisüberwachungen* sammeln
- ***Leistungsüberwachungsbenutzer*** können *Leistungsindikatoren* lokal oder remote verwenden
- ***Hauptbenutzer*** dienen zur Abwärtskompatibilität
- ***Remotedesktopbenutzer*** können sich über *Remotedesktop* remote anmelden
- ***Replikations-Operator*** sind für Aufgaben aus dem Bereich der *Dateireplikation* in *AD DS*-Umgebungen vorgesehn

Smartcards speichern digitale Zertifikate die sich zur *mehrstufigen Authentifizierung* eigenen.
Smartcards können den von *Windows 7* unterstützten *PIV*-konformen *Minitreiber* verwenden, was das installieren von Drittanbietersoftware erspart.
Mehrstufige Authentifizierung bedeutet z.B. Zertifikat + Benutzer + Passwort.

Lokale GPO -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Sicherheitsoptionen

- ***Interaktive Anmeldung:*** *Smartcard* erforderlich
- ***Interaktive Anmeldung:*** Verhalten beim Entfernen von *Smartcard* (Arbeitstation Sperren | Abmelden erzwingen | Trennen, falls *Remotedesktopdienst*-Sitzung)

Kontorichtlinien sind *Kenntwort*- und *Kontosperrungsrichtlinien*.

Lokale GPO -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen

- ***Kennwortchronik erzwingen*** N veraltete Kennwörter erreicht das Benutzer nicht nur eine gewisse Anzahl von Kennwörtern benutzen.
- ***Maximales Kennwortalter*** Zeitraum in Tagen
- ***Minimales Kennwortalter*** Zeitraum in Tagen hindert Benutzer daran die *Kennwortchronik erzwingen* Richtlinie zu umgehen
- *Minimale Kennwortlänge* N Zeichen
- ***Kennwort muss Komplexitätsvoraussetzungen*** entsprechen Groß- und Kleinbuchstaben, Ziffern und Symbole, nicht Anmeldename oder Vor- und Nachname entsprechen
- ***Kennwörter mit umkehrbarer Verschlüsselung speichern*** aus Kompertibilitätsgründen für ältere Software; macht die Speicherung unsicherer
- ***Kontosperrungsrichtlinien***
    - *Kontosperrdauer*
    - *Kontosperrungsschwelle*
    - *Zurücksetzungsdauer des Kontosperrungszählers* für die Dauer in der erfolgslose Anmeldungen gelten

Authentifizierungsprobleme bzw. das Zurücksetzen von Kennwörtern können über *Kennwortzurücksetzungsdatenträger* oder das *Zurücksetzen des Kennworts* des Benutzerkontos.

Kennwortzurücksetzungsdatenträger müssen erstellt werden und verhindern das verlieren von verschlüsselten Daten.

Systemsteuerung -> Kennwortrücksetzungsdiskette erstellen

Zurücksetzen des Kennwortes kann nur die lokale Administrator-Benutzergruppe. Beim *Zurücksetzen des Kennwortes* verliert der Benutzer den Zugriff auf *EFS*-verschlüsselte-Dateien, auf persönliche *Zertifikate* und auf Daten im *Windows-Tresor.*

`$mmc compmgmt.msc` *Lokale Gruppen und Konten -> Benutzerkonten*
`$net user <Benutzername> <Kennwort>`

Gesperrte Konten können mit `$mmc compmgmt.msc` *Konto ist geperrt* aufgehoben werden.

EFS-Zertifikate lassen sich nicht von der *Anmeldeinformationsverwaltung* sichern.
EFS-Zertifikate lassen sich mit der *Zertifikate-Konsole* `certmgr.msc`, mit dem Tool *Dateiverschlüsselungszertifikate verwalten* oder dem Befehlszeilentool `cipher` sichern.
EFS-Zertifikate lassen sich in eine *PFX-Datei* exportieren oder sichern.
PFX-Dateien lassen sich importieren oder auf dem ursprünglichen Computer Wiederherstellen.

```
$mmc certmgr.msc
$cipher /x <Dateiname>.pfx
```

DirectAccess

DirectAccess löst herkömmliche *VPN* (*Virtual Privat Network*) Lösungen über *PPTP* (*Point-to-Point Tunneling Protocol*), *L2TP/IPsec* (*Layer 2 Tunneling Protocol/Internet Protocol Security*) und *SSTP* (*Secure Socket Tunneling Protocol*) ab.

GPO -> Computerrichtlinien -> Administrative Vorlagen -> Netzwerk -> TCP/IP-Einstellungen -> IPv6-Übergangstechnologien

Grundlagen

- *IPv6-VPN*-Verbindung, geschützt durch IPsec
- verfügbar sobald eine Internetverbindung besteht
- bidirektional, Client-Server und Server-Client Kommunikation möglich
- kombinierbar mit *NAP* (*Network Access Protection*), *Windows-Updates*, *Gruppenrichtlinienupdates*, *Software-Updates*
- *Verbindungssicherheitsrichtlinien*
- Konfiguration über *GPO*

Voraussetzungen

- *Windows 7 Enterprise* oder *Ultimate*
- Benutzer muss einer speziellen *DirectAccess-Sicherheitsgruppe* angehören
- *Computerzertifikate* zur beidseitigen Authentifizierung
- *DirectAccess*-Server (*Windows 2008 R2 Server*), *DNS*-Server, *AD DS*

DirectAccess-Verbindungsaufbau

i. Herstellung der *Internetverbindung* (meist vor dem Anmelden)
ii. *Netzwerkidentifikationsphase* prüft ob die *DirectAccess-IntranetWebsite* erreichbar ist
iii. Falls kein Kontakt zur *DirectAccess-IntranetWebsite*; prüfen ob ein IPv6-Netzwerk vorliegt
iv. Falls *IPv6-Netzwerk* vorliegt; Client verbindet sich mit seiner *Öffentlichen-IPv6-Adresse* direkt zum *DirectAccess-Server*
v. Keine *IPv6-Netzwerk*; Client *IPv6-über-IPv4-Tunnel* (*IP6-zu-IP4* oder *Teredo*)
vi. Kein Tunnel weil *Firewall* oder *Proxy*; Verbindungsaufbau via *HTTPS*. *IP-HTTPS* kapselt *IPv6*-Datenverkehr in *HTTPS*.
vii. *DirectAccess-IPsec-Sitzung* wird eingerichtet nach der *Authentifizierung* über *Comptuterzertifikate*
viii. *DirectAccess-Server* prüft *AD DS* ob Computer und Benutzer autorisiert sind für eine Verbindung via *DirectAccess*

Client-Nertzwerkverbindung	***DirectAccess-Verbindungsmethode***
Öffentliche IPv6-Adresse	*Öffentliche IPv6-Adesse*
Öffentliche IPv4-Adresse	*IP6-zu-IP4*
Private IPv4-Adresse (NAT)	*Teredo*
Firewall oder Proxy	*IP-HTTPS*

```
$netsh interface ipv6 set teredo enterpriseclient <IPv4-
Adresse>
$netsh interface 6to4 set relay <IPv4-Adresse>
$netsh interface httpstunnel add interface client
https://FQDN/IPHTTPS
```

Virtual Privat Network

VPN (*Virtuel Privat Network*) ermöglicht Verbindungen über das Internet zu Remotenetzwerken.

Lokal GPO -> Benutzerkonfiguration -> Administrative Vorlagen -> Netzwerk -> Netzwerkverbindung

Netzwerk- und Freigabencenter -> Neue Verbindung oder neues Netzwerk einrichten -> Verbindung mit dem Arbeitsplatz herstellen

***VPN*-Protokoll Aufbau**

- *Datenvertraulichkeit* (Verschlüsselung)
- *Datenintegrität*
- *Schutz vor Wiedergabeangriffen*
- *Datenursprungsauthentifizierung*

***VPN*-Protokolle** (Sortiert nach steigender Sicherheit)

- ***PPTP*** (*Point-to-point Tunneling Protocol*)
  - Kein *PKI* (*Public Key Infrastructure*)
  - Authentifizierung *via MS-CHAP, MS-CHAPv2, EAP* und *PEAP*
  - Verschlüsselung *MPPE*
  - Datenvertraulichkeit
  - Keine Datenintegrität
  - Keine Datenursprungsauthentifizierung
- ***L2TP/IPsec*** (*Layer 2 Tunneling Protocol/Internet Protocol Security*)
  - *PKI* (Zertifikatsdienstinfrastruktur)
  - Datenursprungsauthentifizierung auf Paketbasis
  - Datenintegrität
  - Datenvertraulichkeit
  - Schutz vor Wiedergabeangriffen
- ***SSTP*** (*Secure Socket Tunneling Protocol*)
  - Kabselt PPP-Datenverkehr über den SSL-Kanal des HTTPS-Protokolls
  - Datenursprungsauthentifizierung
  - Datenintegrität
  - Datenvertraulichkeit
  - Schutz vor Wiedergabeangriffen (relay)
- ***IKEv2***
  - *IPv6*
  - Unterstützt *VPN-Reconnect*
  - Authentifizierung via geschütztes *EAP* (*Protected Extensible Application Protocol*), gesichertes Kennwort (*EAP-MS-CHAPv2*) und *MS Smartcard* und andere *Zertifikate* (*PKI*)
  - Datenursprungsauthentifizierung
  - Datenintegrität
  - Datenvertraulichkeit
  - Schutz vor Wiedergabeangriffen

VPN-Authentifizierungs-Protokolle

- ***PAP*** (*Password Authentication Protocol*) nur für ältere *VPN*-Server
- ***CHAP*** (*Challenge Authentication Protocol*) ebenfalls Kennwortbasis, wird nicht vom *Windows 2008 Server* unterstützt
- ***MS-CHAPv2*** (*Microsoft Challenge Handshake Authentification Protocoll Version 2*) auf Kennwortbasis (zur Authentifizierung des momentan angemeldeten Benutzers)
- ***PEAP/PEAP-TLS*** (*Protected Extensible Authentication Protocol with Transport Layer Securtiy*) auf Zertifikatbasis
- ***EAP-MS-CHAPv2/PEAP-MS-CHAPv2*** auf Kennwortbasis , zertifizierter *VPN*-Server (einziges Kennwortbasiertes Protokoll das mit IKEv2 zusammenarbeitet)
- *Smartcard-* oder *andere Zertifikate*

VPN-Reconnect funktioniert mit *PPTP*, *L2TP/IPsec* oder *SSTP* und dient zur Wiederherstellung einer *VPN-Sitzung* bei Unterbrechungen wie dem Wechsel der *Öffentlichen-IP*.
VPN-Reconnect verwendet *IKEv2-Tunnelprotokolle* und die *MOBIKE*-Erweiterung die zulässt, dass das ändern der Internetadresse des *VPN*-Clients ohne erneute Authentifizierung möglich ist.
Nur *Windows Server R2* unterstützt *IKEv2*.

NAP (*Network Access Protection*) oder ***Netzwerkzugriffsschutz*** ist eine *Windows Server 2008* Technologie die auf Basis einer Integritätseinstufung des Clienten einschränken kann.
NAP hindert nicht konforme Clients am Zugriff auf das Netzwerk.
NAP kann für Clients im *LAN* aber auch für *VPN*-Clients, *Remotegateway-* und *DirectAccess*-Clients aktiviert werden.

***NAP*-Konfiguration**

- *Antivierensoftware* auf dem Client installiert?
- *Antispywaresoftware* auf dem Client installiert?
- *Windows-Firewall* auf dem Client aktiviert?
- *Automatische Windows-Updates* aktiviert?
- *Softwareupdates* auf dem Client installiert?

Aktionen: *Client Warten* (*Wartungsnetzwerk*, *WSUS, GPO-Updates* etc.); *Client Abweisen und Zugriff sperren*

Windows-Sicherheitsintegritätsprüfung -> Richtlinieneinstellungen für die Windows-Sicherheitsintegritätsprüfung auswählen

Remotedesktopdienst (*Terminaldienst*) sind Remotedesktopsitzungen von einem Client auf einen Server.

Remotedesktopgateway (*Terminaldienstgateway*) sind Remotedesktopsitzungen von einem Client aus dem Internet auf einen Server (ohne *VPN*).

Remotedesktopverbindung -> Erweitert -> Verbindung von überall aus herstellen -> Einstellungen -> Remotedesktop-Gatewayservereinstellung

Lokale GPO -> Benutzerkonfiguration -> Administrative Vorlagen -> Windows-Komponenten -> Remotedesktopdienste -> Remotedesktopgateway

- Authentifizierung für Remotedesktop festlegen
- Verbindung über Remotedesktopgateway aktivieren
- Adresse des Remotedesktop-Gatewayservers festlegen

RemoteApp ermöglicht es Anwendungen, die auf dem *Remotedesktopdiensteserver* ausgeführt werden, ihre Bildschirmausgabe auf den *Remotedesktopclients* anzuzeigen.
RemoteApps können zum Startmenü hinzugefügt werden.
RemoteApps können auch über das Internet ausgeführt werden wenn dies in den Einstellungen für die RemoteApp-Bereitstellung aktiviert ist.
RemoteApps lassen sich über *GPO* oder *Remotedesktop-Verknüpfungen* (`.rdp`) verteilen.

Überwachen von *Remoteverbindungen* über Anmelde- und Abmeldeüberwachungsrichtlinien.

Lokale GPO -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Überwachungsrichtlinien -> Anmeldeereignisse überwachen

Lokale GPO -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Sicherheitsoptionen -> Überwachung: Unterkategorie der Überwachungsrichtlinien

Lokale GPO -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Sicherheitsoptionen -> Erweiterte Überwachungsrichtlinienkonfiguration -> Systemüberwachungsrichtlinien -> Anmelden/Abmelden

BitLocker

- *BitLocker* ist unter *Windows 7 Ultimate* und *Enterprise* verfügbar.
- *BitLocker* verschlüsselt *Volumen* vollständig.
- *BitLocker* mach die Daten eines verschlüsselten *Volumens* erst zugängig wenn die Integrität des Startsystems geprüft wurde.
- *BitLocker* überprüft die Integrität mit Hilfe eines Verschlüsselungsschlüssels der in der *Systempartition* des Rechners abgelegt ist und *der Windows-Authentifizierung.*
- *BitLocker* schütz vor *Offlineangriffen*.
- *BitLocker* schütz nicht vor *Lokalen*- oder *Netzwerkangriffen*

***BitLocker*-Modi**

- **Nur *TPM*** (*Trusted Platfrom Module*) benötigt keine zusätzliche Authentifizierung
- ***TPM* mit *Startschlüssel*** erfordert *USB-Laufwerk* mit vorkonfiguriertem *Startschlüssel* auf einem *USB*-Datenträger, dass das System starten kann
- ***TMP* mit *PIN*** erfordert die Eingabe eines *PINs* um das System zu starten
- ***TMP* mit *Startschlüssel* und *PIN***
- ***BitLocker* ohne *TPM*** bietet keinen Schutz der Startumgebung und benötigt ein *USB*-Laufwerk mit vorkonfiguriertem *Startschlüssel* auf einem *USB*-Datenträger (für Computer ohne *TPM-Chip*).

Lokale GPO -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Richtlinien für öffentliche Schlüssel -> BitLocker-Laufwerksverschlüsselung -> Betriebsystemlaufwerke -> Zusätzliche Authentifizierung beim Start anfordern (auch ohne TPM zulassen)

TPM-Chips (*Trusted Platform Module Chips*) lassen sich über die *TPM-Verwaltungskonsole* verwalten.

```
$mmc tpm.msc
$gpupdate

$manage-bde

$manage-bde -status
$manage-bde -SetIdentifier <Volumen:> (Volumen soll DRA unterstützen)
$manage-bde -protectors –get <Volumen:>
$manage-bde -unlock <Volumen:> -Certificate –ct
<Zertifikatsfingerabdruck> (Volumen Wiederherstellen)
```

BitLocker To Go ist *BitLocker* für *Wechseldatenträger*.
BitLocker To Go braucht keinen *TPM*.
BitLocker To Go Wechseldatenträger können mit einem Passwort geschützt werden.
BitLocker To Go in Windows 7 läst sich zu Vorgängerversionen in soweit unterscheiden, dass *Wechseldatenträger* die mit *BitLocker To Go* verschlüsselt wurden auch von anderen Computern gelesen werden können.
BitLocker To Go braucht unter *Windows Vista* und *XP* ein *BitLocker To Go-Lesetool*

Lokale GPO -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Richtlinien für öffentliche Schlüssel -> BitLocker-Laufwerksverschlüsselung -> Wechseldatenträger

- *Verwenden von BitLocker auf Wechseldatenträgern steuern*
- *Smartcard-Verwendung für Wechseldatenträger konfigurieren*
- *Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind*
- *Zugriff auf BitLocker-geschützte Wechseldatenträger von früheren Windows-Versionen zulassen*
- *Kennwortverwendung für Wechseldatenträger konfigurieren*
- *Festlegen, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden können*

Datenwiederherstellungsagenten (*Data Recovery Agents, DRAs*) sind Benutzerkonten zur Wiederherstellung von verschlüsselten Daten.
DRAs können von *BitLocker* verschlüsselte *Volumen*, falls der *PIN* oder der *Startschlüssel* verloren geht.
DRAs können sämtliche *BitLockervolumen* einer Organisation wiederherstellen wenn *Eindeutige IDs für Organisation angeben* in den *GPOs* aktiviert wurde.

Lokale GPO -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Richtlinien für öffentliche Schlüssel -> BitLocker-Laufwerksverschlüsselung

- *Eindeutige IDs für Organisation angeben*
- *Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können*
- *Festlegen, wie BitLocker-geschützte Festplattenlaufwerke wiederhergestellt werden dürfen*
- *Festlegen, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden dürfen*

Mobilität

Offlinedateien sind Ordner und Dateien aus freigegebenen Ordnern die lokal zwischengespeichert werden, damit diese auch ohne direkte Verbindung zur Netzwerkressource verfügbar sind.
Offlinedateien sind in den Windows *7-Editionen Professional, Enterprise* und *Ultimate* verfügbar.
Wenn Dateien für den Offlinezugriff freigegeben sind, speichert *Windows 7* eine Kopie der Datei in einem lokalen Zwischenspeicher.
Windows 7 synchronisiert selbständig *Offlinedateien*.
Konflikte werden mit dem *Synchronisationscenter* gelöst.
Offline verfügbare Dateien werden im *Windows-Explorer* mit dem Status *Immer verfügbar* angezeit

Datei (Rechte Maustaste) -> Immer online verfügbar machen

Offlinedateien **Betriebsarten**

- ***Onlinemodus*** werden Änderungen an der Datei zuerst in der *Dateifreigabe* gespeichert und dann im lokalen Zwischenspeicher übernommen. Die Synchronisation erfolgt automatisch oder manuell.
- ***Automatischer Offlinemodus*** werden Netzwerkfehler erkannt wechselt *Windows 7* in den automatischen *Offlinemodus*. Dateioperationen erfolgen an der lokalen Kopie im Zwischenspeicher. *Windows 7* versucht alle 2 Minuten automatisch eine Verbindung herzustellen. Kommt eine Verbindung zustande wechselt *Windows 7* in den *Onlinemodus*.
- ***Manueller Offlinemodus*** wird durch die Schaltfläche *Offlinebetrieb* im *Windows-Explorer* aktiv. Soll der Computer wieder in den *Onlinemodus* wechseln muss ein klick auf *Oblinebetrieb* im *Windows-Explorer* erfolgen.
- ***Modus für langsame Verbindungen*** ist unter *Windows 7* standardmäßig aktiviert und wird eingesetzt, wenn die Übertragungsrate im Netzwerk unter den Standardwert von *64 KB/sec* fällt. Dieser Wert lässt sich über die *GPOs* ändern. Fällt der Wert unter 64KB/sec. geht *Windows 7* in den *Offlinemodus*, steigt er wieder wechselt *Windows 7* wieder in den *Onlinemodus*.

Lokale GPO -> Computerkonfiguration -> Administrative Vorlagen -> Netzwerk -> Offlinedateien

- *Vom Administrator zugewiesene Offlinedateien*
- *Hintergrundsynchronisierung konfigurieren (Modus für langsame Verbindungen)*
- *Maßnahmen bei der nicht standardmäßigen Serververbindungstrennung*
- *Offlinedateicache verschlüsseln*
- *Modus für langsame Verbindungen konfigurieren*
- *Übertragungsrate für langsame Verbindungen konfigurieren*

Transparenter Zwischenspeicher speichert Kopien aller Dateien die ein Benutzer aus einem *freigegebenen Ordner* öffnet auf einem lokalen Volumen zwischen.
Transparenter Zwischenspeicher ist nicht verfügbar wenn die Verbindung zur *freigegebenen Ressource* unterbrochen ist.
Transparenter Zwischenspeicher versucht nicht die lokale Datei synchron zu halten zum Orginal auf dem *Remoteserver*.
Transparenter Zwischenspeicher funktioniert bei allen Dateien aus einer *freigegebenen Ressource*, nicht nur denjenigen die offline verfügbar sein sollen.
Transparenter Zwischenspeicher lässt sich auf Computern verwenden die kein Mitglied einer *Domäne* sind.
Transparenter Zwischenspeicher ähnelt *BranchCache*.

Lokale GPO -> Computerkonfiguration -> Administrative Vorlagen -> Netzwerk -> Transparentes Zwischenspeichern aktivieren

Unterschied zwischen *Transparentem Zwischenspeicher* und *BranchCache*

- *Transparenter Zwischenspeicher* wird nicht verteilt oder gemeinsam genutzt
- *Transparenter Zwischenspeicher* ist auch unter *Windows 7-Edition Professional* verfügbar, nicht nur unter *Ultimate* und *Professional*
- *Transparenter Zwischenspeicher* müssen nicht die freigegebenen Ordner auf einem *Windows Server 2008 R2* gehostet sein.

Offlinedateiausschlüsse ist eine *Richtlinie* in der bestimmte Dateitypen nicht mehr offline verfügbar sind.

Lokale GPO -> Computerkonfiguration -> Administrative Vorlagen -> Netzwerk -> Dateien aus der Zwischenspeicherung ausschließen

Synchronisationscenter dient zur dazu *Offlinedateien* zu verwalten und *Synchronisationskonflikte* manuell zu lösen.
Synchronisationskonflikte treten auf wenn sowohl die *Offlinedatei* im lokalen Zwischenspeicher als auch die Datei auf dem Dateiserver geändert wurde.
Synchronisationskonflikte lassen sich im *Synchronisationscenter* anzeigen und beheben.
Das *Synchronisationscenter* bietet einen Dialog um zu entscheiden welche Version der Datei behalten werden soll.

- *Die lokale Version behalten*
- *Die Serverversion behalten*
- *Beide Versionen behalten*

Ordner -> Eigenschaften -> Freigabe -> Erweiterte Freigabe -> Zwischenspeicher -> Offlineeinstellungen

Energiesparpläne sind Sammlungen von Einstellungen, die festlegen, wie ein Computer unter *Windows 7* Strom verbraucht.

```
$powercfg
$powercfg (-import | -export)
$powercfg (-deviceenablewake | -devicedisablewake)
<Gerätename>
$powercfg devicequery (wake_from_any | wake_armed)
$powercfg –energy && start energy-report.html
```

Systemsteuerung -> Energieoptionen

Lokale GPO -> Computerverwaltung -> Administrative Vorlagen -> System -> Energieverwaltung

- *Verhindern des automatischen Energiesparmodus für Anwendungen zulassen*
- *Automatischen Energiesparmodus bei geöffneten Netzwerkdateien zulassen*
- *Wechseln in den Energiesparmodus durch Anwendungen zulassen*

*(Alle weiteren Richtlinien sind wie **in Erweiterte Energieeinstellungen für Energiesparpläne**)*

Vordefinierte *Energiesparpläne*

- *Höchstleistung*
- *Ausbalanciert* (Standardeinstellung nach der Installation)
- *Energiesparmodus*

Energieoptionen lässt sich festlegen was beim drücken des *Netzschalters* und der *Energiespartaste* oder *Zuklappen* passieren soll.

- *Energie sparen*
- *Ruhezustand*
- *Herunterfahren*
- *Nichts unternehmen*

***Energieeinstellungen* Modi**

- ***Energiesparmodus*** ist der Prozessor und der größte teil der *Systemgeräte* ausgeschalten. Das *RAM* des Computer bleibt eingeschalten das geöffnete Anwendungen und Dokumente erhalten bleiben. *USB*-Mäuse, Tastatur und *NIC* bleiben ebenfalls eingeschalten. Wird der Computer nicht mit der Tastatur oder Maus geweckt wechselt er in den *Ruhezustand*.
- ***Hybrider Energiemodus*** soll den Stromverbrauch von Desktopcomputern senken, die nicht über eine *USV* verfügen. Wenn ein Desktopcomputer im *Energiesparmodus* läuft und eine Unterbrechung der Stromversorgung auftritt, kann Datenverlust erfolgen. Der Inhalt im *RAM* bleibt in diesem Modus erhalten und wird in spezielle Dateien auf die Festplatte geschrieben.
- ***Ruhezustand*** werden alle *Geräte* ausgeschalten und Inhalte des *RAMs* werden in spezielle Dateien auf dem *Betriebssystemvolumen* geschrieben. Ein Computer der sich im *Ruhezustand* befindet kann mit dem *Netzschalter* eingeschaltet werden.
- ***Herunterfahren*** bleiben Inhalte des *RAMs* nicht erhalten und alle *Geräte* werden ausgeschalten.

Erweiterte Energieeinstellungen* für *Energiesparpläne

- *Kennwort beim Reaktivieren anfordern*
- *Festplatte auschalten nach* N min.
- *Desktophintergrundeinstellungen* (Animierte Hintergründe)
- *Drahtlosverbindungen* (*Drahtlosnetzwerkadapter*-Einstellungen die sich auf seine Leistung auswirken)
- *Energie sparen* (Einstellungen für den Wechsel in den *Energiesparmodus* oder Ruhezustand)
    - *Deaktivierung nach* N min.
    - *Hybriden Standbymodus zulassen*
    - *Ruhezustand nach* N min.
    - *Zeitgeber zur Aktivierung zulassen*
- *USB-Einstellungen*
- *Netzschalter und Zuklappen*
- *PCI-Express* (PCI Express Link State Power Management)
- *Prozessorenergieverwaltung*
- *Bildschirm*
- *Multimediaeinstellungen*
    - *Bei der Freigabe von Medien* (z.B. *Bibliotheken* als Netzwerkressource)
    - *Bei der Videowiedergabe*
    - *Batterie*

Windows Update

Windows Update ist das wichtigste Werkzeug zum Verwalten von *Softwareupdate* von *Windows 7-Clients*.
Benutzer mit *Administratorenberechtigung* können nach Updates suchen, Einstellungen für Updates ändern, installierte Updates überprüfen und ausgeblendete Updates anzeigen.
Ein Benutzer der seine *Rechte nicht anheben* kann, kann Updates installieren.
Windows Update verwendet den *Dienst Windows Update* der standardmäßig jeden Tag um 3 Uhr Nachts nach Updates sucht. Ist der Computer ausgeschalten sucht er nach Updates nach dem nächsten Einschalten.
Windows Update-Dateien sind nach folgendem Muster aufgebaut:

```
windows<windows-version>-<KB-Nr.>-<Architectur>.msu
windows6.1-kb123456-x86.msu
```

```
$wuauclt
$wuauclt /detectnow
```

```
$wusa <Volume:\path\to\file.msu> /quit /norestart
```

Systemsteuerung -> Windows Update

Lokale GPO -> Computerkonfiguration -> Administrative Vorlagen -> Windows-Komponenten -> Windows Update

- *Optionen „Updates installieren und herunterfahren“ im Dialogfeld „Windows herunterfahren“ nicht anzeigen*
- *Die Standartoption „Updates installieren und herunterfahren“ im Dialogfeld „Windows herunterfahren“ nicht anpassen*
- *Windows Update-Energieverwaltung aktivieren, um das System zur Installation von geplanten Updates automatisch zu reaktivern*
- *Automatische Updates konfigurieren*
    - *Vor Herunterladen und Installation benachrichtigen*
    - *Autom. Herunterladen, aber vor Installation benachrichtigen*
    - *Autom. Herunterladen und laut Zeitplan installieren*
    - *Lokale Administrator[en] ermöglichen, Einstellung auszuwählen*
    - *Installationstag und Installationszeit*
- *Internen Pfad für den Microsoft Updatedienst angeben*
- *Suchhäufigkeit für automatische Updates*
- *Nichtadministratoren gestatten, Updatebenachrichtigungen zu erhalten*
- *Softwarebenachrichtigungen aktivieren*
- *Automatische Updates sofort installieren*
- *Empfohlene Updates über automatische Updates aktivieren*
- *Keinen automatischen Neustart für geplante Installationen automatisch Updates durchführen, wenn Benutzer angemeldet sind*
- *Erneut zu einem Neustart für geplante Installation auffordern*
- *Neustart für geplante Installationen verzögern*
- *Zeitplan für geplante Installation neu erstellen*
- *Clientseitige Zielordnung aktivieren* (WSUS Clientcomputer Gruppen)

- *Signierte Updates aus einem Intranetspeicherort für Microsoft-Updatedienste zulassen*

***Update* Gruppen**
- *Wichtige Updates* (beheben meist kritische Sicherheitslücken)
- *Empfohlene Updates* (beheben meist Funktionsprobleme)
- *Optionale Updates* (Treiberupdates und Sprachpakete)

Systemsteuerung -> Windows Updates -> Einstellungen ändern

- *Updates automatisch installieren (empfohlen)*
- *Updates herunterladen, aber Installation manuell durchführen*
- *Nach Updates suchen, aber Zeitpunkt zum Herunterladen und Installieren manuell festlegen*
- *Nie nach Updates Suchen (nicht empfohlen)*
- *Empfohlene Updates auf die gleiche Weise wie wichtige Updates bereitstellen*
- *Alle Benutzern das Installieren von Updates auf diesem Computern ermöglichen*

Updateverlauf
- Listet alle Updates die auf dem Computer mit oder ohne Erfolg installiert worden
- Listet das *Installationsdatum* und die *Klassifikation* auf
- Zeigt die *KnowledgeBase-Kennung* (KB123456)
- Zeigt weitere Informationen zu dem Update beim klick auf das selbige

Installierte Updates
- Kurze allgemeine Bezeichnung
- *KnowledgeBase-Kennung*

Updates deinstallieren
- Installierte Updates zeig die *KnowledgeBase-Kennung* die zum deinstallieren nötig ist
- Deinstallierte Updates müssen *Ausgeblendet* werden da sie sonst beim nächsten Update reinstalliert werden

Updates für andere Microsoft-Produkte
Systemsteuerung -> Windows Updates -> Updates für weitere Microsoft-Produkte

Updates mit einem Proxyserver
- Verwenden von *Web Proxy Auto Detect* (*WPAD*)
- Verwenden des Befehlszeilentools netsh um Proxyoptionen zu importieren

```
$netsh winhttp import proxy source=ie
```

WSUS (*Windows Server Update Service*) kann *Windows* und *Microsoft Updates* bereitstellen die mit *Windows Update* abgerufen werden.
WSUS muss mit *Version 3.0 Service Pack 1* auf dem *Updateserver* bereitgestellt werden um mit *Windows 7-Clients* zusammenzuarbeiten.
WSUS erlaubt es den *Updateverlauf* und den *Updatezeitraum* selbst zu bestimmen um Updates vorher auf Kompatibilität zu testen.
WSUS erlaubt es Gruppen von *Clientcomputern* zu erstellen um Updates selektiv oder stufenweise zu verteilen.
WSUS erlaubt auch die zentrale deinstallation eines Updates.

Wartungscenter ist der zentrale Ort um die Anzeige von Problemen aus dem Bereich Sicherheit und Wartung.
Wartungscenter-Meldungen erscheinen als *Sprechblase* auf der *Taskleiste*.
Wartungscenter benötigt den *Dienst Sicherheitscenter*.
Benutzer aus der Gruppe *Administratoren* können das *Wartungscenter* konfigurieren und festlegen welche Meldungen angezeigt werden.
Wartungscenter zeigt Meldungen aus den folgenden Bereichen an:

- *Windows Update*
- *Internet-Sicherheitseinstellungen*
- *Firewall*
- *Schutz vor Spyware und ähnlichen Schutzmaßnahmen*
- *Benutzerkontensteuerung (UAC)*
- *Virenschutz*
- *Windows-Sicherung*
- *Windows-Problembehandlung*

Systemsteuerung -> Wartungscenter

Microsoft Baseline Security Analyzer (*MBSA*) kann überprüfen ob auf einem Client alle erforderlichen Updates installiert sind.
MBSA kann auch überprüfen ob es Probleme mit der *Sicherheitskonfiguration* eines Computers gibt.
MBSA kann nicht nur Clients sondern auch Server überprüfen.
MBSA braucht Adminsitratorrechte.

Internet Explorer

Kompatibilitätsansicht im *Internet Explorer* kann Websites die für Vorgänger des *Internet Explorers* 8 geschrieben wurden darstellen, indem man das *Zerrissene Seite Symbo*l am Ende der *Adressleiste* anklickt.
Kompatibilitätsansicht kann für *Alle Websites in Kompatibilitätsansicht anzeigen* eingestellt werden.
Kompatibilitätsansicht ist automatisch aktiviert für Websites *der Zone Lokales Intranet*.

Internet Explorer -> Menu Extras -> Einstellungen für die Kompatibilitätsansicht

Lokale GPO -> Computerkonfiguration -> Administrative Vorlagen \ Windows-Komponenten -> Internet Explorer -> Kompatibilitätsansicht

Lokale GPO -> Benutzerkonfiguration -> Administrative Vorlagen \ Windows-Komponenten -> Internet Explorer -> Kompatibilitätsansicht

- *Internet Explorer 7-Standards-Modus aktivieren*
- *Kompatibilitätsansicht deaktivieren*
- *Schaltfläche „Kompatibilitätsansicht“ deaktivieren*
- *Aktualisierte Websitelisten von Microsoft einbeziehen*
- *Richtlinienliste von Internet Explorer 7-Sites verwenden*

Sicherheitseinstellungen

- *Lokales Intranet Sites in der Zone Lokales Intranet*
- *Vertrauenswürdige Sites in der Zone Vertrauenswürdige Sites*
    - *Websites die erhöhte Rechte benötigen*
    - *Standard-Sicherheitsstufe ist Mittel*
    - *Vertrauenswürdige Site werden im Dialogfeld Vertrauenswürdige Sites hinzugefügt*
    - *Standardeinstellung ist das Sites nur zu Vertrauenswürdige Sites hinzugefügt werden können wenn sie mit einem SSL-Zertifikat versehen sind*
- *Eingeschränkte Sites*
    - *Potenziell böswillige Websites*
    - *Standard-Sicherheitsstufe ist Hoch*
    - *Geschützer Modus des Internet Explorers ist standardmäßig aktiviert*
- *Internet*
    - *Umfasst alle Websites die nicht in den anderen Sicherheitsstufen enthalten sind*
    - *Standart-Sicherheitsstufe ist Mittelhoch*
    - *Geschützer Modus des Internet Explorers ist standardmäßig aktiviert*
    - *Das Anzeigen persönlicher Daten aus anderen Websites ist blockiert*
    - *Keine Änderungen an Windows 7 durch Websites erlaubt*

Sicherheitsstufen wirken restriktiv. Sie Steuern Verhalten von *Active-X-Steuerelementen*, *Skripting* und Einstellungen für *Benutzerauthentifizierung.*

Standard-Sichheitsstufen

- *Mittel*
- *Mittelhoch*
- *Hoch*

Individuelle-Sichheitsstufen kann man festlegen wie *Zertifikatsprüfungen* durchgeführt werden, *SmartScreen-Filter* konfigurieren oder welche *TLS*, *SSL* Versionen zulässig sind.

SmartScreen-Filter ist ein Feature von *Internet Explorer*, dass das öffnen von Websites verhindert, bei denen bekannt ist, dass sie Malware verteilen.
SmartScreen-Filter ist also ein *Antiphishing-Filter*.
SmartScreen-Filter schützen vor folgenden Techniken:

- Analysiert besuchte Websites draufhin, ob sie verdächtige Merkmale enthalten
- Vergleicht die besuchten Sites mit einer regelmäßigen aktualisierten Liste bekannter Phishing- und Malwaresites
- Prüft heruntergeladene Dateien auf bekannte Malware

SmartScreen-Filter warnt oder blockiert gefährliche Websites und Downloads.

InPrivate-Modus besteht aus zwei Technologien: *InPrivate-Filterung und InPrivat-Browsen*.
InPrivate-Modus ist eine Datenschutztechnologie.

InPrivate-Browsen legt fest welche Daten vom Browser gespeichert werden.
InPrivate-Browsen zeigt ein Symbol in der Adressleiste an, wenn es aktiviert ist.
InPrivate-Browsen löscht anfallende *Sitzungsdaten*, wenn der Browser geschlossen wird

Internet Explorer -> Menu Sicherheit -> InPrivate-Browsen

InPrivate-Filterung schränkt ein, welche Daten von *Browsersitzungen* von Dritten verfolgt werden können.
InPrivate-Filterung hindert auch *Add-Ons* am Datensammeln.

Internet Explorer -> Menu Sicherheit -> InPrivate-Filterung
Internet Explorer -> Menu Sicherheit -> Einstellungen der InPrivate-Filterung

Lokale GPO -> Computerkonfiguration -> Administrative Vorlagen -> Windows Komponenten -> Internet Explorer -> InPrivate

- *InPrivate-Filterung deaktivieren*
- *InPrivate-Browsen deaktivieren*
- *Keine InPrivate-Filterungdaten sammeln*
- *Symbolleisten und Erweiterungen beim Starten des InPrivate-Browsens deaktivieren*
- *Schwelle für InPrivate-Filterung* (Wert N der verschiedenen Websites mit eingebetteten Conten des Anbieters X)

Add-Ons erweitern den Funktionsumfang von *Internet Explorer* um:

- *Symbolleisten und Erweiterungen*
- *Suchanbieter* (Schnellsuche)
- *Schnellinfos* (accelerator – erscheinen wenn Inhalte markiert werden)
    - *Bloggen* (Ausgewählte Informationen direkt bloggen)
    - *E-Mail* (Ausgewählte Informationen in E-Mail versenden)
    - *Karte* (Ausgewählte Information in einem Kartendienst anzeigen)
    - *Übersetzen* (Ausgewählte Information übersetzen)
- *InPrivate-Filterung*

Add-Ons lassen sich installieren und deinstallieren aber auch deaktivieren und aktivieren.
Add-Ons lassen sich von Standardbenutzern hinzufügen sofern dies die GPO zulassen.

Internet Explorer -> Menu Extras -> Add-Ons Verwalten

Lokale GPO -> Computerkonfiguration -> Windows-Komponenten -> Internet Explorer -> Schnellinfos
Lokale GPO -> Benutzerkonfiguration -> Windows-Komponenten -> Internet Explorer -> Schnellinfos

- *Nicht standardmäßige Schnellinfos bereitstellen*
- *Standardschnellinfos bereitstellen*
- *Schnellinfos deaktivieren*
- *Richtlinienschnellinfos verwenden*

Internet Explorer-Einstellungen zurücksetzen
Internetoptionen -> Erweitert -> Zurücksetzen

Internet Explorer-Sicherheitseinstellungen zurücksetzen
Internetoptionen -> Sicherheit -> Alle Zonen auf Standartstufe zurücksetzen

Internet Explorer Inhaltsratgeber filtert *Websites*(-Inhalte) aus, nach bestimmten Kriterien wie *Sexuel Content* oder *Alterbegrenzung*
Internet Explorer Inhaltsratgeber verhindert den Zugriff auf ungefilterte *Websits* in den *Standardeinstellungen*

Popupblocker verhindert das Website ungewollt neue Browser-Fenster öffnen.
Popupblockersicherheitsstufen funktionieren ähnlich wie *Browser-Sicherheitsstufen*.
Popupblocker blockiert keine Sites die in der Sicherheitszone *Lokales Internet* oder *Vertrauenswürdige Sites* liegen, sowie Websites für die *Ausnahmen* definiert wurden.

Internet Explorer -> Menu Extras -> Popupblockereinstellungen

SSL-Zertifikate dienen dazu die Identität einer Website zu prüfen und den Datenverkehr zwischen Website und Benutzer zu verschlüsseln.
Website die mit *SSL-Zertifikaten* geschützt sind, zeigen ein *goldenes Schlosssymbol* in der *Adressleiste*.

Goldenes Schlosssymbol -> Websiteidentifizierung -> Zertifikate

Falls Probleme mit einem *SSL-Zertifikat* auftreten zeigt *Internet Explorer* eine Warnung.
Der Benutzer kann nun entscheiden wie er fortfahren möchte:

- *Klicken Sie hier, um diese Webseite zu schließen*
- *Laden dieser Website fortsetzen (nicht empfohlen)*

In folgenden Fällen können Probleme mit einem *SSL-Zertifikat* auftreten:

- *Websiteadresse stimmt nicht mit der Adresse des Zertifikats überein*
- *Websitezertifikat wurde gesperrt*
- *Websitezertifikat ist nicht mehr gültig*
- *Websitezertifikat stammt nicht aus einer vertrauenswürdigen Quelle* (Selfsign)
- *Probleme mit dem Sicherheitszertifikat*

```
$inetcpl.cpl
```

Internetoptionen -> Inhalt -> Zertifikate

SSL-Zertifikate Importieren oder Exportieren

Internetoptionen -> Inhalte -> Zertifikate -> Herausgeber

Leistungsüberwachung

Bei ***Leistungsüberwachung*** geht es darum Leistung zu überwachen und zu optimieren, mögliche Leistungsengpässe zu identifizieren und die erforderlichen Ressourcen aufzurüsten.
Um Leistungsdaten zu überwachen muss ein (Remote-)Benutzer mindestens in den Gruppen *Leistungsüberwachungsprotokollbenutzer* und *Ereignisprotokollleser* sein.

`$perfmon` -> *Überwachungstools -> Leistungsüberwachung*
Systemsteuerung -> Leistungsinformationen und –tools -> Leistungsüberwachung öffnen

Leistungsindikatoren kann man mit dem Plus-Symbol für Objekte wie *Arbeitsspeicher* oder *TCPv4* (und Unterobjekten wie *Aktive Verbindungen* oder *Verbindungsfehler*) hinzugefügt.

`$perfmon` -> *Überwachungstools -> Leistungsüberwachung -> Eigenschaften*

- *Allgemein* (Aktualisierungsrate, Anzeigeoptionen)
- *Quelle* (Echtzeit oder Protokolldateien)
- *Daten* (Leistungsindikatore und deren Konfiguration und Darstellung)
- *Grafik* (Darstellungseigenschaften für Datendiagramme, Grafen und Berichte)
- *Darstellung* (Darstellungseigenschaften für das Systemmonitorfenster)

Sammelsätze (*Data Collector Set, DCS*) stellen *Systeminformationen* zusammen und speichern sie in einer Datei.

Vordefinierte Sammelsätze zeichnen in der Standarteinstellung 10min. lang Daten auf. System Diagnostics nur 1min.

- ***System Performance*** (*Systemleistung*)
  - Einsatz: Leistungseinbrüche, langsame Computer
  - Leistungsindikatoren: Prozessor-, Datenträger-, Arbeitsspeicher- und Netzwerkleistungsindikatoren
- ***System Diagnostics*** (*Systemdiagnose*)
  - Einsatz: Zuverlässigkeitsprobleme, problematische Hardware, Treiber- oder Abbruchfehlern
  - Leistungsindikatoren: wie System Performance und detaillierte Systeminformationen

`$perfmon` -> *Sammelsätze -> System* (rechte Maus-Taste *start*)

Nachdem ein Sammelsatz erstellt wurde kann der Bericht unter `$perfmon` -> *Berichte* eingesehen werden.

Sammlungen können Benutzerdefinierte Aktionen Durchführen. Skripte oder Programme können z.B. ausgeführt werden.

`$perfmon` -> *Sammelsätze -> Benutzerdefiniert -> Neu -> Sammlung*

```
$logman
$logman create (counter | trace | config | alert) <my_title> …
$logman (start | stop | delete) <my_title>
```

Mit *Sammlung* können folgende *Sammlungstypen* hinzugefügt werden:

- ***Leistungsindikatorensammlung***
  - Leistungsstatistiken über längere Zeiträume
  - Baselineanalysen
- ***Ereignisablaufverfolgungssammlung***
  - Systemereignisse
- ***Konfigurationssammlung***
  - Systemzustand, Registrierschlüssel und WMI-Verwaltungspfade
- ***Leistungsindikatorenwarnung***
  - Warnungen die ausgelöst werden wenn Leistungsindikatoren einen bestimmten Schwellwert über- oder unterschreiten

Systemdiagnosebericht auch *Computerintegritätsprüfung* liefert Details und Status von *Hardwareressourcen*, *Systemreaktionszeit* und *Prozessen* auf dem lokalen Computer sowie *Systeminformationen* und *Konfigurationsdaten.*

```
$runas /user:Administrator “perfmon /report“
```

Zuverlässigkeitsüberwachung verfolgt die Stabilität eines Computers auf einem *Stabilitätsindex* von 1 bis 10.
Je mehr Fehler oder Neustarts auf einem Computer stattfinden, desto niedriger ist der *Stabilitätsindex*.
Zuverlässigkeitsüberwachung liefert Informationen welche Änderungen auf einem System vorgenommen wurden.
Zuverlässigkeitsüberwachung zeichnet die *Stabilitäts*- und *Zuverlässigkeitsereignisse* eines Jahres auf. Das *Stabilitätsdiagramm* zeigt Daten über einer Datumsachse an.
Zuverlässigkeitsüberwachung eignet sich um sporadisch auftretende Probleme zu diagnostizieren. Z.B. eine installierte Anwendung die ab und zu dazu führt, dass das System Abstürzt.

```
$perfmon /rel
```

Stabilitätsindex basiert auf Daten, die über die gesamte Lebensdauer eines Systems gesammelt werden.
Stabilitätsindex Indexwert wird über die letzten 28 Tage berechnet.
Aktuelle Fehler wirken sich stärker auf den *Stabilitätsindex* aus als länger zurück liegende.
Da erst nach 28 Tagen eine zuverlässige *Baseline* vorhanden ist, wird der *Stabilitätsindex* davor als gepunktete Linie dargestellt.

Stabilitätsdiagramm zeigt eine Kurve des *Stabilitätsindex* an, wobei für jeden Tag ein Abschnitt eingeteilt ist.
Symbole in der unteren Hälfte des Diagrams stehen für *Zuverlässigkeitsereignisse*.
Zuverlässigkeitsereignisse beziehen sich entweder auf die *Stabilitätsmessung* des Systems oder auf *Software Installation* und *Deinstallation*.

Wartungscenter meldet Probleme aus dem Bereich *Sicherheit*, *Wartung* und *zugehörigen Einstellungen*, die helfen, die *Gesamtleistung* eines Computers zu ermitteln.
Wartungscenter benachrichtigt Benutzer, wenn z.B. Probleme mit der *Firewall*, *Antivirensoftware*, *Antispywaresoftware* oder *Windows Update* auftreten.
Wartungscenter Benachrichtigungen erscheinen als Meldung im *Infobereich* der *Taskleiste*.
Wartungscenter Benachrichtigungen können über die Einstellung *Wartungscentereinstellungen ändern* ausgeschalten und konfiguriert werden.
Wartungscenterstatus eines Elements ändert seine Farbe, je nach Schweregrad der Meldung, von grün nach rot.

Systemsteuerung -> System und Sicherheit -> Wartungscenter

Windows-Leistungsindex basiert aus Archivierten Daten des *Wartungscenters* und gibt die aktuelle *Leistung* eines Computers auf dem Index von 1 bis 7,9 an.
Windows-Leistungsindex misst die Fähigkeit der *Hardware*- und *Softwarekonfiguration* eines Computers.
Jede *Hardwarekomponente* enthält eine separate *Teilnote*, die in die Gesamtbewertung eingeht.
Teilnoten für Hardwarekomponenten wie *Prozessor*, *Arbeitsspeicher*, *Grafik* und *primäre Festplatte* werden angezeigt

Systemsteuerung -> System und Sicherheit -> Wartungscenter -> Leistungsinformationen anzeigen

Task-Manager

```
$taskmgr
```

Registrierkarte	Funktion
Leistung	*CPU*- und *Arbeitsspeicherbelastung*
Prozesse	Zeigt Laufende *Prozesse* an. Diese können beendet oder die *Priorität* verändert werden
Dienste	Zeigt Laufende *Dienste* an. Diese können gestartet oder beendet werden. Dienste können zu *Prozessen* verändert werden
Netzwerk	Zeigt die Laufende *Netzwerkauslastung* an
Benutzer	Zeigt auf dem System angemeldete Benutzer an. Benutzer können getrennt werden

Task-Manager kann auch die ***Priorität*** von *Prozessen* festlegen in den Stufen: *Echtzeit, Hoch, Höher als normal, Normal, Niedriger als Normal, Niedrig*

Task-Manager kann auch die ***Prozessorzugehörigkeit*** konfigurieren mit *Zugehörigkeit festlegen* wenn mehrere Kerne und/oder Prozessoren vorhanden sind.

Ressourcenmonitor zeigt Informationen in Echtzeit zu *Hardware*- und *Softwareressourcen* an.
Ressourcenmonitor-Ergebnisse können nach *Prozessen* oder *Diensten* gefiltert werden.
Ressourcenmonitor kann *Dienste* und *Prozesse*, starten, beenden, anhalten und fortsetzen oder *Anwendungen* analysieren die nicht mehr reagieren.
Ressourcenmonitor-Sitzungen lassen sich Speichern und verwalten.
Ressourcenmonitor hat fünf Registrierkarten*: Übersicht, CPU, Arbeitsspeicher, Datenträger* und *Netzwerk*.
Ressourcenmonitor-Registrierkarten zeigt in der *Übersicht* eine Liste aller laufenden *Prozesse*. Hier können Prozesse ausgewählt werden für die in den anderen *Registrierkarten* ausführliche Information angezeigt werden sollen.

```
$resmon
```

Task-Manager -> Prozesse -> Ressourcenmonitor

Process Explorer zeigt an welche *Handles* und *DLLs* ein Prozess geöffnet oder geladen hat.
Process Explorer ist nicht im Lieferumfang von *Windows 7* enthalten, er muss im *Microsoft Technet* unter http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx heruntergeladen werden.
Process Explorer kann als *Ressourcenmonitor* verwendet werden, um festzustellen, welche Anwendung für Aktivitäten auf der Festplatte verantwortlich ist und auf welche Ordner und Dateien zugegriffen wird.
Process Explorer zeigt auch Systeminformationen, Verlauf der CPU-Auslastung, zugeordneten virtuellen Arbeitsspeicher und den I/O-Durchsatze an.

Ereignisanzeige zeigt *Ereignisprotokoll* an.
Ereignisprotokolle sind Dateien die *Ereignisse* auf dem Computer aufzeichnen, z.B. *Benutzeranmeldungen* oder *Fehlermeldungen*.
Ereignisse werden in folgende Kategorien eingesteilt:

- *Kritisch*
- *Fehler*
- *Warnung*
- *Informationen*

Sicherheitsprotokoll enthält zwei weitere Kategorien:

- *Erfolgsüberwachung*
- *Fehlerüberwachung*

```
$eventvwr
```

Ereignisanzeige kann *benutzerdefiniert Ansichten* erstellen, verschiedene *Quellprotokolle* oder *Ereignisse* können durchsucht und gefiltert werden.
Ereignisanzeigen Ansichten sind dauerhaft, *Filter* hingegen Sitzungsabhängig.
Ereignisanzeige zeichnet Informationen in verschiedenen Protokollen auf. *Windows-Protokolle* sind:

- ***Anwendung*** speichert *Programmereignisse*
  - Schweregrad: *Fehler, Warnung* oder *Information*
- ***Sicherheit*** speichert sicherheitsrelevante *Überwachungsereignisse*
  - Unterteilt in: erfolgreiche oder fehlgeschlagene Operationen
  - Beispiel: *Erfolgsüberwachung* der *Benutzeranmeldung*
- ***System*** speichert *Systemereignisse* von Windows 7 und Systemdiensten
  - Schweregrad: *Kritisch, Fehler, Warnung* oder *Information*
- ***Weitergeleitete Ereignisse*** speichert *Ereignisse*, die von andren Computer weitergeleitet werden

Filter anhand des *Ereignistyps*, *Vorgegebene Filter* Bsp.:

`eventvwr` -> *Ereignisanzeige* -> *Anwendungs- und Dienst-Protokolle* -> Microsoft -> Windows -> *Diagnostics-Performance*

Systemsteuerung -> Leistungsinformationen und –tools -> Weitere Tools -> Leistungsdetails im Ereignisprotokoll

Anwendungs- und Dienstprotokolle sind Protokolle für Programme und Dienste die auf dem Computer laufen.
Folgende Protokolle können vorhanden sein:

- *Hardwareereignisse*
- *Internet Explorer*
- *Key Management Service*
- *Media Center*
- *Eine große Zahl von Microsoft Windows-Protokollen*
- *Microsoft Office-Diagnose*
- *Microsoft Office-Sitzung*
- *Windows-PowerShell*

Verknüpfen von Aufgaben mit Ereignissen ermöglicht das Ausführen eines Programms oder Skript, versenden einer E-Mail oder Benachrichtigungen, wenn ein bestimmtes *Ereignis* eintritt.

Bsp. Für *Aufgabe an dieses Ereignis* anfügen …:

`eventvwr` -> *Ereignisanzeige -> Windows-Protokolle -> Sicherheit* -> Rechtsklick *Ereignis -> Aufgabe an dieses Ereignis anfügen …*

Ereignisweiterleitung (*event forwarding*) überträgt alle *Ereignisse*, die ein bestimmtes Kriterium erfüllen, an einen Remotecomputer (*Sammelcomputer*). Sammelcomputer verwalten *Ereignisse* verschiedener Computer in einem zentralen *Ereignisprotokoll*.
Ereignisweiterleitung arbeitet via *HTTP* (*Hypertext Transfer Protocol*) oder via *HTTPS* (*Hypertext Transfer Protocol Secure*) um *Ereignisse* von einem *Quellcomputer* an einen *Sammelcomputer* zu senden.
Ereignisweiterleitungsverkehr ist immer verschlüsselt, sowohl über *HTTPS* als auch über *HTTP*.
Ereignisweiterleitung ist abhängig von den *Diensten Windows-Remoteverwaltung* (*WS-Verwaltung*) und *Windows-Ereignissammlung*.
Ereignisweiterleitung braucht zudem die passenden *Windows-Firewall-Ausnahmen* auf Port 80, bzw. 443.

Abonnements unterscheiden sich in *sammlungsinitiierten* (*collector-initiated*) und *quellinitiierte* (*source-initiated*).
Sammlungsinitiierte Abonnements rufen der *Sammelcomputer Ereignisse* auf den *Quellcomputern* ab.
Sammlungsinitiierte Abonnements eignen sich für bekannte und überschaubare anzahlen von Rechnern.

Sammelcomputer
`$wecutil qc`

Quellcomputer
`$winrm quickconfig`
`$mmc compmgmt.msc` *Computer-Konto der Lokale Administratoren oder Ereignisprotokollleser Gruppe hinzufügen*

Quellinitiierte Abonnements sendet der *Quellcomputer* (*Quellcomputer*) *Ereignisse* an den *Sammelcomputer*.
Quellinitiierte Abonnements eignen sich bei einer großen Anzahl von Rechnern.
Quellinitiierte Abonnements können jederzeit neue *Quellcomputer* hinzugefügt werden.
Quellcomputer können beim *Quellinitiierten Abonnement* auch als *Weiterleitungscomputer* bezeichnet werden.

Weiterleitungscomputer
`$winrm qc -q`
`$mmc gpedit.msc` *Computerkonfiguration -> Administrative Vorlagen -> Windows-Komponenten -> Ereignisweiterleitung -> Serveradresse, Aktuelisierungsintervall und Ausstellerzertifizierung eines Abonnement-Managers (SubscriptionManager) -> Eigenschaften -> SubscriptionManager -> Anzeigen ->* Quellcomputer hinzufügen
`$gpudate /force /wait:0`

Sammelcomputer
```
$wecutil qc -q
$wecutil cs configuration.xml
```

MSconfig (*Systemkonfiguration*) dient in erster Linie dazu, Probleme beim Startvorgang von *Windows* zu untersuchen.
MSconfig ändert welche Programme beim Systemstart ausgeführt werden, bearbeitet *Konfigurationsdateien* und ermöglicht *Windows-Dienste* zu steuern und *Windows-Leistungs- und Problembehandlungswerkzeuge* aufzurufen.
MSconfig kann *Startoptionen* festlegen und einen *Diagnosesystemstart* ausführen, bei dem nur ein Basissatz von Treibern, Programmen und Diensten geladen wird.
MSconfig kann auf der Registrierkarte Start die Quelle der *Startdatei* aussuchen und als *Standarteintrag* speichern.

```
$msconfig
```

Dienste Konsole, ein *MMC-Snap-In*, listet die Selben *Dienste* wie *MSconfig* (*Systemkonfiguration*) in der *Registrierkarte Dienste* auf.
Dienste Konsole liefert Informationen zu jedem Dienst und bietet erweiterte Konfigurationsmöglichkeiten.

```
$mmc services.msc
```

Dienst -> Eigenschaften

- ***Allgemein*** zeigt an ob ein *Dienst* läuft und legt den *Starttyp* fest : *Automatisch, Automatisch (Verzögert), Manuell und Deaktiviert*
- ***Anmelden*** legt fest unter welchem *Benutzerkonto* sich ein *Dienst* anmeldet. Im Normalfall wird ein Dienst im *lokalen Systemkonto* angemeldet
- ***Wiederherstellen*** legt fest welche *Aktionen* ausgeführt werden wenn ein *Dienst* abstürzt. Es können Aktionen für den ersten, zweiten und weitere Fehler konfiguriert werden. Als Aktionen kann das ausführen von Programmen oder der Neustart des Rechners gewählt werden
- ***Abhängigkeiten*** zeigt alle *Dienste*, *Systemtreiber* und *Startreihenfolgegruppen* die ein *Dienst* benötigt

WMI (*Windows Management Instrumentation*) stellt *Modelle* der verwalteten Umgebung als *WMI-Klassen* zur Verfügung um auf *Systemverwaltungsinformationen* zugreifen.
WMI-Klassen beschreiben *Eigenschaften* von *verwalteten Ressourcen*.
Verwaltete Ressourcen ist irgendeine *Objekt* (*Computerhardware, Computersoftware, Dienste oder Benutzerkonten*) das mit Hilfe von *WMI* verwaltet wird.
WMI kann genutzt werden um eigene Tools für die *Leistungsmessung* zu schreiben und die Ausgabe von *Systeminformationen* zu regeln.

WMI-Skriptingbiliotheken erlauben das schreiben von *WMI-Skripten* in:

- *VB-Script (Microsoft Visual Basic Scripting Edition)*
- *Microsoft Jscript*
- *WSH (Windows Script Host)*
- *ActivePerl*

WMI-Skripte können zur Konfiguration von Windows eingesetzt werden, aber auch Ereignisse reagieren und agieren.

Folgendes *WMI-Skript* in *VB-Script* greift auf *Instanzen* der *Klasse Win32_Battery* zu und gibt den Wert des *Attributs EstimatedChargeRemaining* aus:

```
strComputer = “.“
Set objSWbemService = GetObject(“winmgmts:\\“ & strComputer)
Set colSWemObjectSet =
objSWbemServices.InstancesOf(“Win32_Battery”)
For Each objSWbemObject In colSWbemObjectSet
     Wscript.Echo “Verbleibende Kapazität: “ &
objSWbemObject.EstimatedChargeRemaining & “ Prozent.”
Next
```

Leistungsoptionen ist ein *Leistungs- und Analysetool* in *Windows 7*.

Systemsteuerung -> Leistungsinformationen und –tools -> Weitere Tools -> Darstellung und Leistung von Windows anpassen

- *Visuelle Effekte*
  - *Optimale Einstellung Automatisch Wählen*
  - *Für Optimale Darstellung anpassen*
  - *Für Optimale Leistung anpassen*
  - *Benutzerdefiniert*
- *Erweitert*
  - *Prozessorzeitplanung* (*Hintergrunddienste* oder *Programme*)
  - *Virtueller Arbeitsspeicher/Auslagerungsdateien*
- *Datenausführungsverhinderung* (*Data Execution Prevention, DEP*) verhindert das Arbeitsspeicher auf falsche Weise benutzt wird für wichtige Windowsprogramme und Dienste oder für alle Programme und Dienste

Schreibcache für Festplatten verwendet schnelles *RAM*, um Schreibbefehle, die Daten an Speichergeräte senden, zu sammeln und zwischenzuspeichern, bis das langsamere *Speichermedium* (*Festplatte* oder *Flashspeicher*) sie verarbeiten kann.

<Gerätename> -> Eigenschaften -> Richtlinien

Bsp. *USB*: *Schnelles entfernen* (Deaktiviert die *Schreibcache*) oder *Bessere Leistung* (Aktiviert die *Schreibcache*). Bei Festplatten kann in den *Schreibcacherichtlinien* auch noch der *Schreibcachebuffer* aktiviert bzw. deaktiviert werden um Datenverlust beim Stromausfall zu verhindern.

WPT (*Windows Performance Toolkit*) enthält *Leistungsanalysetools*, die im *Windows SDK* (*Software Development Kit*) für *Windows 7*, *Windows Server 2008* und *Microsoft .NET Framework 3.5* neu eingeführt wurden.
WPT wurde entworfen um *System-* und *Anwendungsleistung* zu messen.
WPT analysiert unter anderem *Anwendungsstartzeiten*, *Systemstartprobleme*, *DPCs* (*Deffered Procedure Call*), *ISRs* (*Interrupt Service Request*), Probleme mit der *Systemreaktionszeit*, Auslastung von *Anwendungsressourcen* und *Interruptwellen*.
WPT ist im *SDK* enthalten und kann im *Microsoft Downloadcenter* heruntergeladen werden.
WPT umfasst folgende Tools:

- Trace Capture, Processing, and Command-Line Analysis Tool (xperf)
  Xperf verwaltet die Endpunkt-zu-Endpunkt-Operationen, die nötig sind, um eine Ablaufverfolgungsdatei für Analysezwecke zu generieren
  - Ereignisablaufverfolgung (Event Tracing for Windows, ETW)
  - Abbild- und Symbolidentifizierung
  - Ablaufverfolgungsspeicherung
  - Unterstützung für Nachbearbeitung
- Visual Trace Analysis Tool (xperfview)
  Xperfview zeigt Informationen, einer mit xperf generierten, au seiner Ablaufverfolgungsdatei an.
- On/Off Transition Trace Capture Tool (xbootmgr.exe)
  Xbootmgr kann folgende Phasen aufzeichnen:
  - Systemstart
  - Herunterfahren
  - Umschalten in den Standbymodus und Aufwecken
  - Umschalten in den Ruhezustand und Aufwecken

```
$xperf -on Base+Network -f kernel.etl
$xperf -start UserTrace -on Microsoft-Windows-Firewall -f
user.etl
$xperf -stop UserTrace
$xperf -stop
$xperf .-merge user.etl kernel.etl single.etl
$xperf -i -single.etcl -o c:\mytrace.txt -a dump
```

Datensicherung

Windows 7-Datensicherung nutzt *Schattenkopien*, um einen *Snapshot* anzufertigen. *Snapshots* können auch bei geöffneten Dateien erstellt werden.

Systemsteuerung -> System und Sicherheit -> Sichern und Wiederherstellen

Sicherungsziele

- *Zweites internes Festplattenlaufwerk (NTFS)*
- *Externes Festplattenlaufwerk (NTFS)*
- *DVD*
- *USB-Flashlaufwerk*
- *Netzwerkspeicherort*
- *VHD*

Sicherungsziele die mit *BitLocker* aktiviert sind können nicht verwendet werden.

Sicherungen sollten nicht auf einer separaten Partition der einzigen Festplatte des Computers gespeichert werden, aus Sicherheitsgründen bei Hardwaredefekt. *Sicherungen* die in einen Netzspeicherort erfolgen, müssen für den *Benutzer* die *Freigabe*- und *NTFS-Berechtigung Vollzugriff* für den Netzwerkordner aktiviert sein. Auf *Sicherungen* haben *Administrator vollzugriff*, *Benutzer* nur *lesen*.

Sicherungsdaten (Standard)

- *Datendateien* in *Bibliotheken, Desktop* und *Windows-Standardordnern* von allen Benutzerkonten
- *Systemabbild* (Betriebssystem, Progamme, Treiber und Registrierungseinstellungen)

Windows-Standardordner sind: *AppData, Contacts, Desktop, Downloads, Favorites, Links, Saved Games und Searches*

Sicherungsarten

- *Systemabbild* sichert ein ganzes *Volumen* in einer kompremierten *.vhd*-Datei. *Datensicherung und –Wiederherstellung* kann im laufenden Betrieb stattfinden
- *Datensicherung* sichert Dateien und Dokumente in eine kompremierte *.zip*-Datei. *Datensicherungen* sind standardmäßig inkrementell. Es werden keine Systemdateien, Progammdateien, *EFS*-verschlüsselte Dateien, *temporäre Dateien*, Dateien im *Papierkorb* oder *Benutzerprofileinstellungen* gesichert

Sicherungen brauchen *Administratoranmeldeinformationen*, *Wiederherstellungen* hingegen nicht.

Datensicherungen sichern *Ordner* und *Dateien*.
Datensicherung wird auch als *Datei- und Ordnersicherung* bezeichnet.

Datensicherungszeitplan kann nach der ersten manuellen Sicherung automatische inkrementelle *Datensicherungen* planen und verwalten.
Inkrementelle *Datensicherungen* werden automatisch gestartet und gespeichert bis das gewählte Ziellaufwerk voll ist. Ist das Ziellaufwerk voll wird die älteste *Datensicherung* gelöscht um neuen Speicherplatz zu schaffen.

Datensicherungs-Ordnerstruktur wird erstellt wenn zum erstenmal eine *Datensicherung* auf z.B. eine Externe Festplatte erfolgt.

```
Volumen:\<Computername>\Backup Set<Jahr-Monat-Tag>
<Uhrzeit>\backup files 1.zip
```

Datensicherungen erstellen automatisch eine *Katalogdatei*, die das Gesicherte Dateisystem mit Berechtigungen abbildet.

```
Volumen:\<computername>\Catalogs\GlobalCatalog.wbcat
```

Dateisicherungen die wiederhergestellt werden, behalten Dateien die Berechtigung der Ursprünglichen Datei.

Systemabbildsicherungen sichern Systemvolumen Block für Block in eine *.vhd*-Datei.
Systemabbildsicherungen können nicht in ein Flashlaufwerk, DVD oder Bandlaufwerk geschrieben werden.
Systemabbildsicherungsziele müssen *NTFS*-Formatiert sein.
Systemabbildsicherungen sind nach der ersten Sicherung inkrementell, nur eine einzige Version der *Systemabbildsicherung* wird gespeichert.
Systemabbildsicherungen müssen manuell in *Sichern und Wiederherstellen* durchgeführt werden.

```
$wbadmin start backup -backuptarget:Volumen: -include:Volumen:
-quit
```

Systemabbildsicherungszeitplan kann mit Hilfe von `$wbadmin` in einer *Batch*-Datei und der *Windows-Aufgabenplanung* konfiguriert werden.

Systemabbildsicherungs-Ordnerstruktur

```
Volumen:\windowsImageBackup\<Computername>\Backup <Jahr>-
<Monat>-<Tag> <Uhrzeit>\file.vhd
```

Systemabbildsicherung erstellt automatisch den Ordner *Catalog* in dem sich die Dateien *GlobalCatalog* und *BackupGlobalCatalog* befinden, die die Versionen des Abbilds aufzeichnen.
Systemabbildsicherung erstellt zudem die Dateien *MediaID* in *<Computername>,* die das Datenträgerabbild identifiziert

Systemabbildwiederherstellung überschreibt das gesamte *Systemvolumen*.
Systemabbildwiederherstellung wird auch als *vollständige Wiederherstellung* (*complete recovery*) oder *complete PC restore* bezeichnet.
Systemabbildwiederherstellungtools werden nach dem booten von *Windows 7 DVD* im *Debugmodus* geladen (*WinPE* bzw. *Windows RE*).

Systemwiederherstellung (*system restore*) nutzt *Systemwiederherstellungspunkte* (*restore point*), die vom *Computerschutz*, z.B. vor dem Installieren von Anwendungen oder Treibern angelegt werden.
Systemwiederherstellung erstellt automatisch einen *Systemwiederherstellungspunkt*, sodass die *Systemwiederherstellung* rückgängig gemacht werden kann.

Systemwiederherstellungspunkte können auch manuell angelegt werden.
Systemwiederherstellungspunkte können (mit Administratorrechten) ausgewählt und wiederhergestellt werden.
Systemwiederherstellungspunkte sichern und ändern keine Benutzerdaten.
Systemwiederherstellungspunkte stellen *Windows-Systemdateien*, -Programme (Skripte) und Registrierungseinstellungen wieder her.
Systemwiederherstellungspunkte werden automatisch alle 7 Tage erstellt, sofern in dieser Zeit kein anderer *Wiederherstellungspunkt* aufgezeichnet wurde.

Systemwiederherstellung-Festplattenplatz kann deaktiviert werden indem man den *Computerschutz* für den betreffenden Datenträger ausschaltet

Computerschutz (*System Protection*) erstellt und speichert regelmäßig Informationen über Systemdateien und Einstellungen eines Computers.
Computerschutz speichert *Vorgängerversionen von Dateien*.
Computerschutz speichert Informationen und Dateien in *Wiederherstellungspunkten* die unmittelbar vor der Installation von Progammen und Gerätetreibern erstellt werden.
Computerschutz wird automatisch aktiviert für das Laufwerk in dem das Betriebssystem installiert ist, wenn dieses Laufwerk *NTFS*-formatiert ist.
Computerschutz reserviert Festplattenplatz für *Wiederherstellungspunkte*, ist der reservierte Festplattenplatz voll, wird der älteste *Wiederherstellungspunkt* gelöscht um wieder Festplattenplatz frei zu geben.

Systemstartoptionen und Systemwiederherstellungsoptionen (F8)

- ***Abgesicherter Modus*** (Minimalsatz an Treibern)
- ***Abgesicherter Modus mit Netzwerktreibern***
- ***Abgesicherter Modus mit Eingabeaufforderung***
- ***Startprotokollierung aktivieren*** (Ntbtlog.txt – Treiberlog)
- ***Anzeige mit niedriger Auflösung aktivieren (640x480)*** (Standard VGA-Treiber für die Grafikkarte)
- ***Letzte als funktionierend bekannte Konfiguration*** (Systemwiederherstellung / Letzte Konfiguration bedeutet: nach dem Abmelden gespeicherter *Wiederherstellungspunkt*)
- ***Verzeichnisdienstwiederherstellung*** (AD DS)
- ***Debugmodus*** (Kerneldebugging und Systemabbildwiederherstellung)
- ***Automatischen Neustart bei Systemfehler deaktivieren***
- ***Erzwingen der Treibersignatur deaktivieren***
- ***Windows normal starten*** (falls der Computer von Installations-DVD gestartet wurde, wird der Setup von Windows-7 geladen)

Systemwiederherstellungsoptionen *(F8) erweiterte Startoptionen ->* ***Debugmodus***

- *Verwenden der Wiederherstellungstools, mit denen sich Probleme beim Starten von Windows beheben lassen*
    - *Betriebssystem wählen* (Falls mehrere Systeme vorhanden sind)
        - ***Systemstartreparatur*** (automatisierte Behebung von Problemen beim Systemstart)
        - ***Systemwiederherstellung*** (*Systemwiederherstellungspunkte*)
        - ***Systemabbild-Wiederherstellung***
        - ***Windows-Speicherdiagnose*** (Arbeitsspeicher-Konsistenz-Prüfung)
        - ***Eingabeaufforderung***
- *Stellen Sie den Computer mithilfe eines zuvor erstellten Systemabbildes wieder her*
    - ***Systemabbildwiederherstellung***

Systemstartoptionen von Windows 7 sind *Startkonfigurationsdaten* und *BCD* die im *BCD-Speicher* abgelegt werden.
Systemstartoptionen können mit `$bcdedit` oder der *WMI-Schnittstelle* verwaltet werden)

`$bootmgr` (Windows-Start-Manager)
`$winload` (Windows-Betriebssystemladeprogramm)
`$winresume` (Windows-Fortsetzungsladeprogramm)

BCD stellt allen *Windows 7*-Computern eine einheitliche Schnittstelle, für das Zuweisen von Rechten zum Verwalten von *Startoptionen*, zur Verfügung.
BCD steht während der Laufzeit und dem Setup zu Verfügung, zudem auch beim Aufwecken eines Computers.
BCD kann mit `$bcdedit` im Remotezugriff verwaltet werden.
BCD kann auch verwaltet werden wenn das System von einem anderen Medium aus gestartet wurde (wichtig wenn ein *BCD-Speicher* wiederhergestellt werden muss).

`$bcedit /set vga on` (erzwingt die Verwendung des *VGA-Anzeigetreibern*)
`$bcedit /debug on` (kerneldebugging für den aktuellen *Betriebssystemstarteintrag*)
`$bcedit /debug <GUID> off` (deaktiviert den *Kerneldebugger* für einen *Betriebssystemstarteintrag*)

`$bcedit` kann zudem folgende Aufgaben ausführen:

- Erstellen eines *BCD-Speichers*
- Neuerstellen eines *BCD-Speichers*
- Hinzufügen von Einträgen zu einem vorhandenen *BCD-Speicher*
- Ändern vorhandener Einträge in einem *BCD-Speicher*
- Löschen von Einträgen aus einem *BCD-Speicher*
- Exportieren von Einträgen aus einem *BCD-Speicher*
- Importieren von Einträgen aus einem *BCD-Speicher*
- Auflisten der momentan aktiven Einstellungen
- Abfragen aller Einträge eines bestimmten Typs
- Übernahme einer globalen Änderung für alle Einträge
- Ändern der Standardwerte für eine Zeitüberschreitung

Wiederherstellen von Vorversionen eines Treibers

- F8 / erweiterte Systemstartoptionen -> Letzte als funktionierend bekannte Konfiguration (Systemwiederherstellungspunkt)
- F8 / erweiterte Systemstartoptionen -> Debugmodus -> Systemwiederherstellung (Systemwiederherstellungspunkte)
- F8 / erweiterte Systemstartoptionen -> Abgesicherter Modus
    - $mmc compmgmt.msc -> Geräte-Manager -> <Gerät> -> Eigenschaften -> Treiber -> Vorheriger Treiber
- F8 / erweiterte Systemstartoptionen -> Anzeige mit niedriger Auflösung aktivieren (640x480)
    - $mmc compmgmt.msc -> Geräte-Manager -> <Gerät> -> Eigenschaften -> Treiber -> Vorheriger Treiber

Wiederherstellen von Dateien und Ordnern

Wiederherstellen von Vorgängerversionen von Dateien und Ordnern stellt der *Volumenschattenkopiedienst* (*Volume Shadow Copy Service, VVS*) als *Schattenkopien* zur Verfügung.

Schattenkopien sind Kopien von Dateien und Ordner die *Windows 7* automatisch speichert.
Schattenkopien (*shadow copy*) werden erstellt wenn ein *Wiederherstellungspunkt* angefertigt wird oder in *Sicherungssätzen* (*Datensicherung*) gesichert wird.
Schattenkopien werden automatisch (mit Standarteinstellungen alle 7 Tage) erstellt, wenn der *Computerschutz* (*Wiederherstellungspunkte*) aktiviert ist.
Schattenkopien stehen nur für *Offlinedateien* zu Verfügung, nicht für *Netzwerkordner*.
Schattenkopien stehen auch nicht für Dateien und Ordner zu Verfügung die *Windows 7* zum ausführen benötigt (*System-Ordner* z.B.).

Volumenschattenkopiedienst (*Volume Shadow Copy Service, VSS*) verwaltet und implementiert *Schattenkopien* und *Volumensnapshots*.
VVS erstellt *Volumensnapshots* wenn eine *Datensicherung* startet. Aus dem *Volumensnapshot* werden die zu sichernden Dateien und Ordner gesichert. Das ermöglicht, dass Dateien und Ordner gesichert werden können, die geöffnet sind oder verwendet werden. Dadurch wird allerdings die Version der Datei gespeichert, die vor dem öffnen existiert hat.

Vorgängerversionen sind entweder *Datensicherungen* von Dateien und Ordnern, die mit der *Konsole Sichern und Wiederherstellen* erstellt wurde und mit demselben Tool oder dem *Assistenten Dateien wiederherstellen* wiederherstellen, oder *Schattenkopien*.
Vorgängerversionen-Wiederherstellungen von Dateien und Ordnern können aus einer *Schattenkopie* oder einer *Datensicherung* erfolgen.
Vorgängerversionen-Wiederherstellungen können eine bisherige Datei überschreiben oder an einem anderen Ort gespeichert werden.
Vorgängerversionen-Wiederherstellungen auch bezeichnet als *Wiederherstellen von Dateien und Ordnern.*

Windows Explorer -> Rechtsklick Datei oder Ordner -> ***Vergängerversion wiederherstellen*** -> Liste der verfügbaren Versionen der Dateien oder Ordners (Die Liste umfasst sowohl Schattenkopien als auch Datensicherungen)

Wiederherstellen von Dateien und Ordnern in einen anderen Speicherort (*kopieren*) wird als *Dummywiederherstellung* (*dummy restore*) bezeichnet.

Systemsteuerung -> Sichern und Wiederherstellen -> Eigene Dateien wiederherstellen

Wiederherstellen umbenannter und gelöschter Dateien

Dateien oder Ordner die gelöscht oder umbenannt wurden können aus einer *Schattenkopie* wiederhergestellt werden, vorausgesetzt der Speicherort der Datei oder des Ordners ist bekannt.
Vorgängerversionen von gelöschten Dateien können nicht direkt wiederhergestellt werden, nachdem der *Papierkorb* geleert wurde. Aber die *Vorgängerversion* des Ordners kann wiederhergestellt werden (dabei sollte aber beachtet werden, dass andere Dateien im Ordner ebenfalls ersetzt werden durch die *Vorgängerversion*).
Falls der *Papierkorb* schon geleert wurde, geht man folgendermaßen vor um gelöschte Dateien und Ordner wiederherzustellen:

1. In welchem Ordner befand sich die gelöschte Datei?
2. *Neuer Ordner* erstellen und den Inhalt des Ordners, der wiederhergestellt werden soll, hineinkopieren
3. Ersetzen des Ordners, der wiederhergestellt werden soll, durch die neuste *Vorgängerversion*
4. Inhalt des aktuellen Ordners in den Ordner mit der *Vorgängerversion* kopieren, mit der Option: *alle älteren Dateiversionen mit neuren Versionen überschreiben* (Die Dateien, die gelöscht wurden, befinden sich nun im Ordner mit der *Vorgängerversion*, wird aber durch die Kopieroperation nicht beeinflusst, weil sie ja im neuen Ordner gar nicht mehr vorhanden ist
5. *Neuer Ordner* kann gelöscht werden

Wiederherstellen mehrerer Vorgängerversionen derselben Datei

Problem: *Vorgängerversionen*, selbst wenn sie nicht am ursprünglichen Speicherort wiederhergestellt werden, überschreiben sich selbst.
Lösung: *Dummywiederherstellung* jeder einzelnen *Vorgängerversion*, wobei nach jeder *Dummywiederherstellung* die *Vorgängerversion* umbenannt werden muss (z.B. in `<Vorgängerversion>_<year>-<month>-<day>-<time>`).

Links und Downloads

http://technet.microsoft.com/

WAIK
http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=de

ACT
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=24da89e9-b581-47b0-b45e-492dd6da2971&displaylang=en

MAP
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=67240b76-3148-4e49-943d-4d9ea7f77730&displaylang=en

MDT
http://www.microsoft.com/downloads/en/details.aspx?familyid=3bd8561f-77ac-4400-a0c1-fe871c461a89&displaylang=en&tm

Process Explorer
http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

Windows Debugging Tools
http://www.microsoft.com/whdc/devtools/debugging/default.mspx

IPv6
http://www.ietf.org/rfc/rfc2373.txt

BOOTP
http://www.ietf.org/rfc/rfc951.txt

DHCP
http://www.ietf.org/rfc/rfc2131.txt

DNS
http://www.ietf.org/rfc/rfc1034.txt
http://www.ietf.org/rfc/rfc1035.txt
http://www.ietf.org/rfc/rfc1591.txt