

## Windows 2008 - BareMetalRecovery

### Inhalt

<b>Windows 2008 - BareMetalRecovery .....</b>	<b>1</b>
<b>1. Vorwort .....</b>	<b>2</b>
<b>2. Vorbereitung einer vollständigen Wiederherstellung – BareMetalRecovery .....</b>	<b>3</b>
<b>3. BareMetalRecovery in einer virtuellen Umgebung.....</b>	<b>3</b>
<b>a. Erstellung einer Virtuellen Maschine .....</b>	<b>3</b>
<b>b. Nachbearbeiten der virtuellen Maschine .....</b>	<b>6</b>
<b>c. Start der virtuellen Maschine .....</b>	<b>8</b>
<b>4. BareMetalRecovery in einer physikalischen Umgebung.....</b>	<b>20</b>
<b>5. Nacharbeiten .....</b>	<b>20</b>
<b>6. Anhang.....</b>	<b>21</b>
<b>a. BSOD 1 – Fehler im Active Directory .....</b>	<b>21</b>
<b>b. BSOD 2 – Inaccessible Boot Device.....</b>	<b>22</b>

## 1. Vorwort

Bei dem dargestellten Server handelt es sich um folgende Konfiguration:

- DELL PowerEdge 2950
  - a. Kaufdatum: 02.10.2008
  - b. CPU: 1x 4C XEON X5450 @ 3GHz
  - c. RAM: 8GB
  - d. HDD: 2x 500GB als RAID1
- Software
  - a. Windows 2008 Server Standard Edition, Service Pack 2
    - i. Domaincontroller
    - ii. DHCP-Server
    - iii. DNS-Server
    - iv. WinS
    - v. Interne Zertifizierungsstelle für PowerShell-Scripte
  - b. Exchange 2007 Standard Edition
  - c. SOPHOS
    - i. Enterprise Console Version 5.2.1.197
    - ii. Pure Message, Version 3.1.3.0
    - iii. Microsoft SQL Server 2008 Express, DaBa für SOPHOS
- Zusätzliche Software
  - a. TeamViewer – Host
  - b. WireShark
  - c. Notepad++
  - d. 7Zip
  - e. KeePass
  - f. Diverse weitere kleine Werkzeuge zur Vereinfachung

Die Sicherung dieser Maschine erfolgt durch die integrierte Windows-Sicherung. Diese Software erlaubt das Wiederherstellen einzelner Dateien aber nicht die Wiederherstellung z.Bsp. einzelner Postfächer oder Emails.

Soll ein bestimmtes Postfach wiederhergestellt werden oder tritt der Super-GAU ein, ist ein s.g. BareMetalRecovery notwendig.

Bei diesem Prozess wird die gesamte Maschine wiederhergestellt. Dies kann in einer virtuellen Umgebung passieren oder auf einem physikalischen Blech. Bei der virtuellen Wiederherstellung wird Hyper-V 3 empfohlen und bei einer physikalischen Wiederherstellung ein möglichst identisches Gerät.

Diese Wiederherstellung dauert, je nach genutzter Hardware, bis zu 5 ½ Stunden.

## 2. Vorbereitung einer vollständigen Wiederherstellung – BareMetalRecovery

Folgende Bedingungen müssen erfüllt sein:

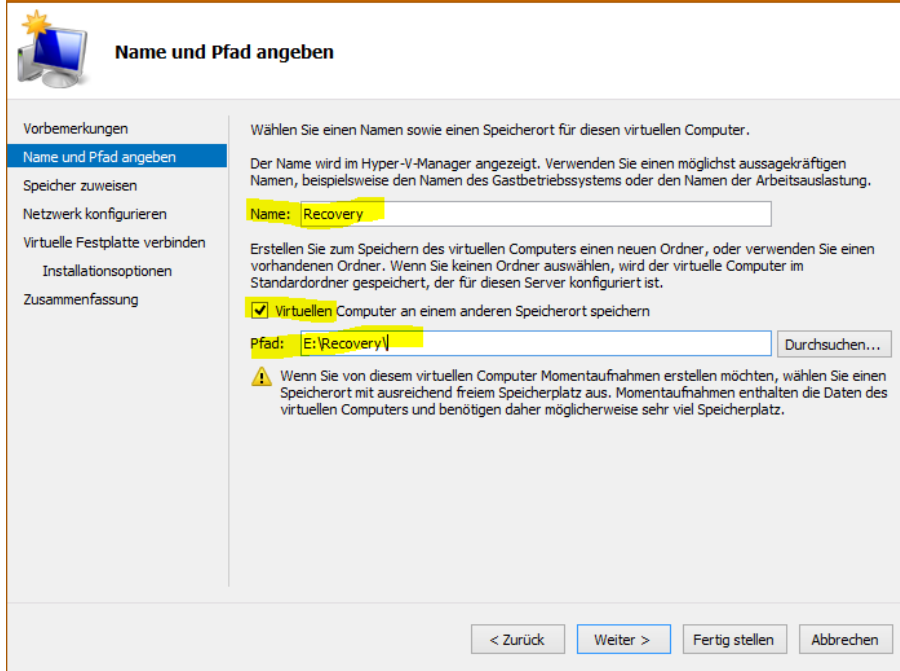
- Das NAS mit dem aktuellsten Backup muss vorhanden und online sein
- Sie haben einen passenden Rechner für die physikalische Wiederherstellung
- Sie haben einen passenden Rechner für die virtuelle Wiederherstellung
- Sie benötigen die Installations-DVD dieses Servers als Scheibe oder ISO
- Sie benötigen einen DHCP-Server

## 3. BareMetalRecovery in einer virtuellen Umgebung

### a. Erstellung einer Virtuellen Maschine

Wiederherstellung unter Verwendung von Hyper-V 3 auf einem Windows 8 Professional.

- Installieren Sie die Hyper-V Rolle und folgen Sie den weiteren Anweisungen
- Öffnen Sie den Hyper-V Manager
- Erstellen Sie eine neue VM auf einem Datenträger mit genügend Platz



**Name und Pfad angeben**

Vorbemerkungen  
Name und Pfad angeben  
Speicher zuweisen  
Netzwerk konfigurieren  
Virtuelle Festplatte verbinden  
Installationsoptionen  
Zusammenfassung


Wählen Sie einen Namen sowie einen Speicherort für diesen virtuellen Computer.  
Der Name wird im Hyper-V-Manager angezeigt. Verwenden Sie einen möglichst aussagekräftigen Namen, beispielsweise den Namen des Gastbetriebssystems oder den Namen der Arbeitsauslastung.

Name:

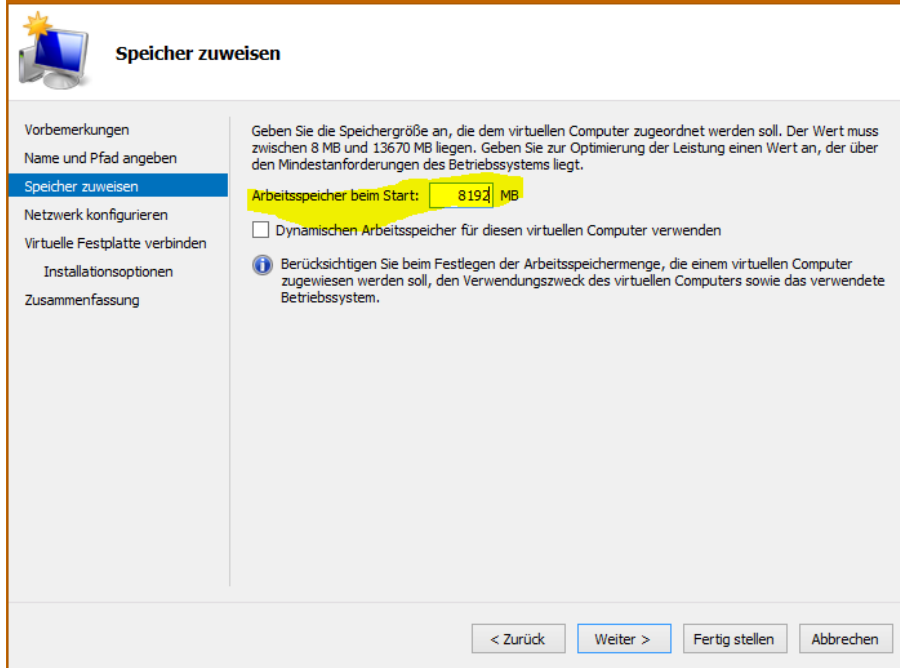
Erstellen Sie zum Speichern des virtuellen Computers einen neuen Ordner, oder verwenden Sie einen vorhandenen Ordner. Wenn Sie keinen Ordner auswählen, wird der virtuelle Computer im Standardordner gespeichert, der für diesen Server konfiguriert ist.

Virtuellen Computer an einem anderen Speicherort speichern

Pfad:

 Wenn Sie von diesem virtuellen Computer Momentaufnahmen erstellen möchten, wählen Sie einen Speicherort mit ausreichend freiem Speicherplatz aus. Momentaufnahmen enthalten die Daten des virtuellen Computers und benötigen daher möglicherweise sehr viel Speicherplatz.

- Vergeben Sie mindestens die gleiche Menge RAM



**Speicher zuweisen**

Vorbemerkungen  
Name und Pfad angeben  
**Speicher zuweisen**  
Netzwerk konfigurieren  
Virtuelle Festplatte verbinden  
Installationsoptionen  
Zusammenfassung

Geben Sie die Speichergröße an, die dem virtuellen Computer zugeordnet werden soll. Der Wert muss zwischen 8 MB und 13670 MB liegen. Geben Sie zur Optimierung der Leistung einen Wert an, der über den Mindestanforderungen des Betriebssystems liegt.

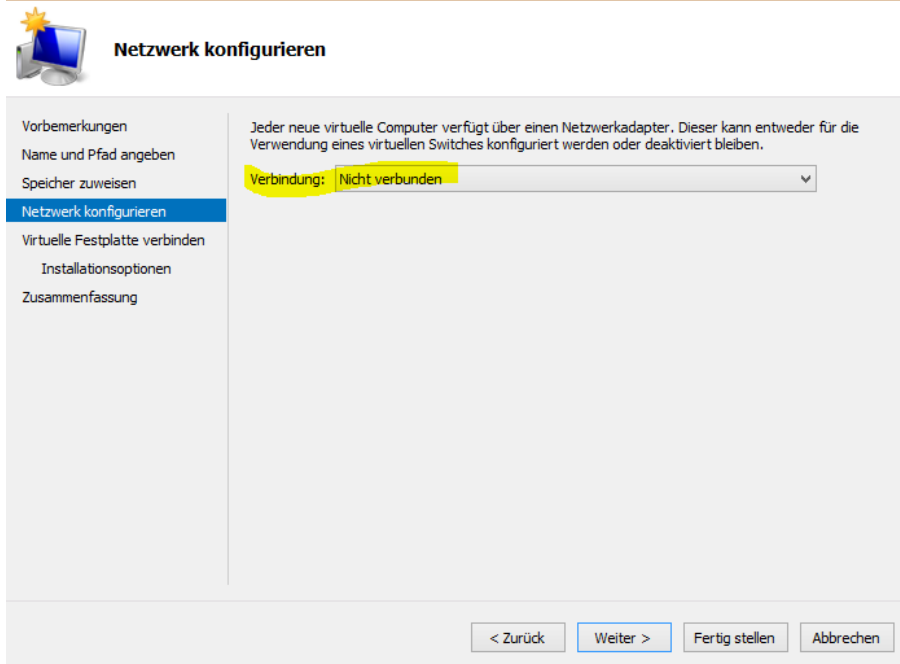
Arbeitsspeicher beim Start:  MB

Dynamischen Arbeitsspeicher für diesen virtuellen Computer verwenden

**i** Berücksichtigen Sie beim Festlegen der Arbeitsspeichermenge, die einem virtuellen Computer zugewiesen werden soll, den Verwendungszweck des virtuellen Computers sowie das verwendete Betriebssystem.

< Zurück Weiter > Fertig stellen Abbrechen

- Die Netzwerkkarte braucht nicht verbunden zu sein, wir müssen später eh noch was ändern.



**Netzwerk konfigurieren**

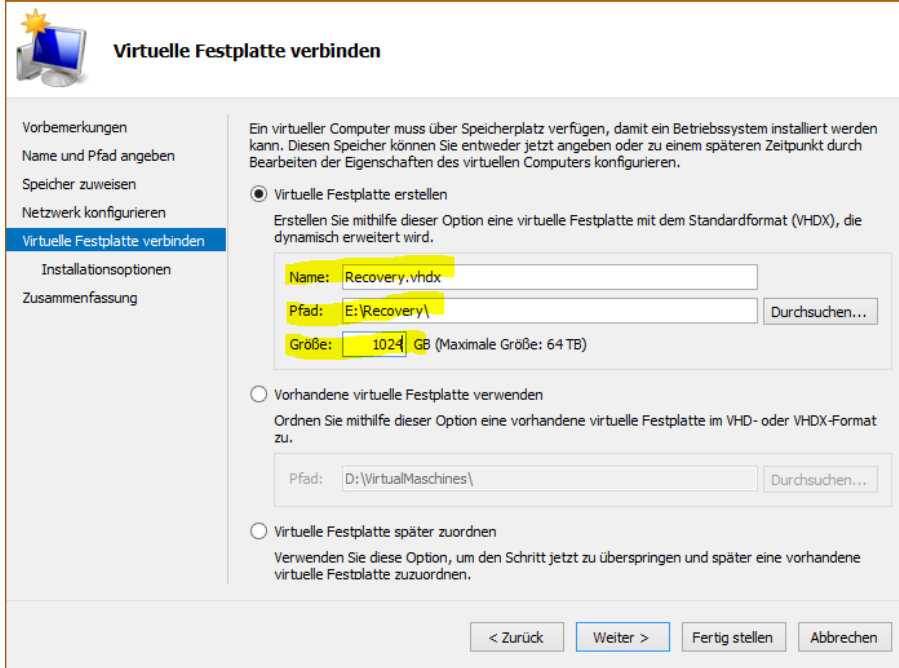
Vorbemerkungen  
Name und Pfad angeben  
Speicher zuweisen  
**Netzwerk konfigurieren**  
Virtuelle Festplatte verbinden  
Installationsoptionen  
Zusammenfassung

Jeder neue virtuelle Computer verfügt über einen Netzwerkkadappter. Dieser kann entweder für die Verwendung eines virtuellen Switches konfiguriert werden oder deaktiviert bleiben.

Verbindung:

< Zurück Weiter > Fertig stellen Abbrechen

- Erstellen Sie einen Datenträger an einer Stelle mit genügend Platz. Als Größe dieses Datenträgers verwende ich das Doppelte des Originals. Da es sich um einen dynamischen Datenträger handelt wird glücklicherweise nur die Datenmenge belegt, die auch nur gebraucht wird.



### Virtuelle Festplatte verbinden

Vorbemerkungen  
Name und Pfad angeben  
Speicher zuweisen  
Netzwerk konfigurieren  
**Virtuelle Festplatte verbinden**  
Installationsoptionen  
Zusammenfassung

Ein virtueller Computer muss über Speicherplatz verfügen, damit ein Betriebssystem installiert werden kann. Diesen Speicher können Sie entweder jetzt angeben oder zu einem späteren Zeitpunkt durch Bearbeiten der Eigenschaften des virtuellen Computers konfigurieren.

Virtuelle Festplatte erstellen  
Erstellen Sie mithilfe dieser Option eine virtuelle Festplatte mit dem Standardformat (VHDX), die dynamisch erweitert wird.

Name: Recovery.vhdx  
Pfad: E:\Recovery\ Durchsuchen...  
Größe: 1024 GB (Maximale Größe: 64 TB)

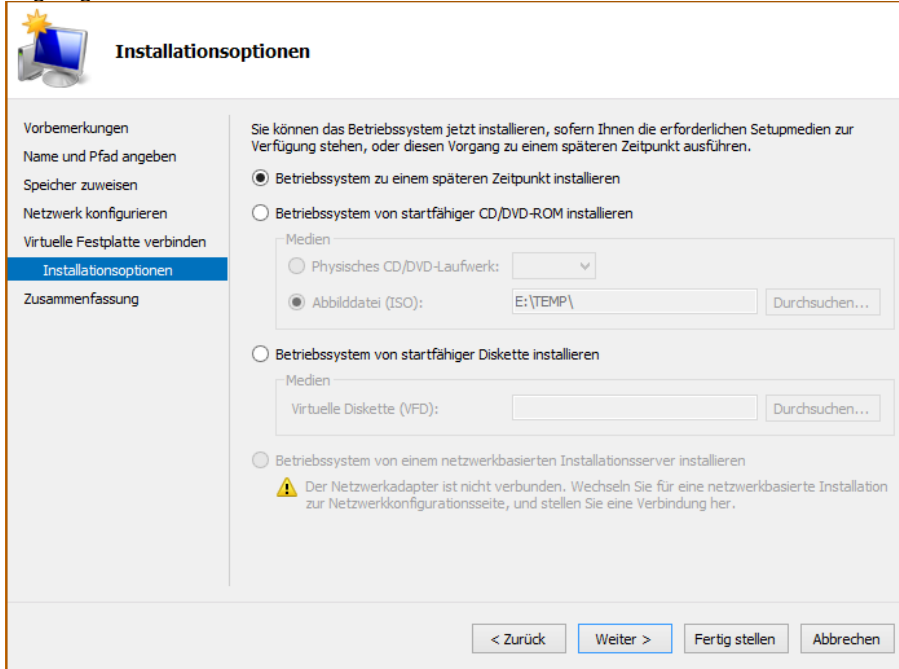
Vorhandene virtuelle Festplatte verwenden  
Ordnen Sie mithilfe dieser Option eine vorhandene virtuelle Festplatte im VHD- oder VHDX-Format zu.

Pfad: D:\VirtualMaschinen\ Durchsuchen...

Virtuelle Festplatte später zuordnen  
Verwenden Sie diese Option, um den Schritt jetzt zu überspringen und später eine vorhandene virtuelle Festplatte zuzuordnen.

< Zurück Weiter > Fertig stellen Abbrechen

- Diese Einstellungen verändere ich nicht. Die ISO-Datei des Betriebssystems wird später angefügt.



### Installationsoptionen

Vorbemerkungen  
Name und Pfad angeben  
Speicher zuweisen  
Netzwerk konfigurieren  
Virtuelle Festplatte verbinden  
**Installationsoptionen**  
Zusammenfassung

Sie können das Betriebssystem jetzt installieren, sofern Ihnen die erforderlichen Setupmedien zur Verfügung stehen, oder diesen Vorgang zu einem späteren Zeitpunkt ausführen.

Betriebssystem zu einem späteren Zeitpunkt installieren


Betriebssystem von startfähiger CD/DVD-ROM installieren

Medien  
 Physisches CD/DVD-Laufwerk: [Dropdown]  
 Abbilddatei (ISO): E:\TEMP\ Durchsuchen...

Betriebssystem von startfähiger Diskette installieren

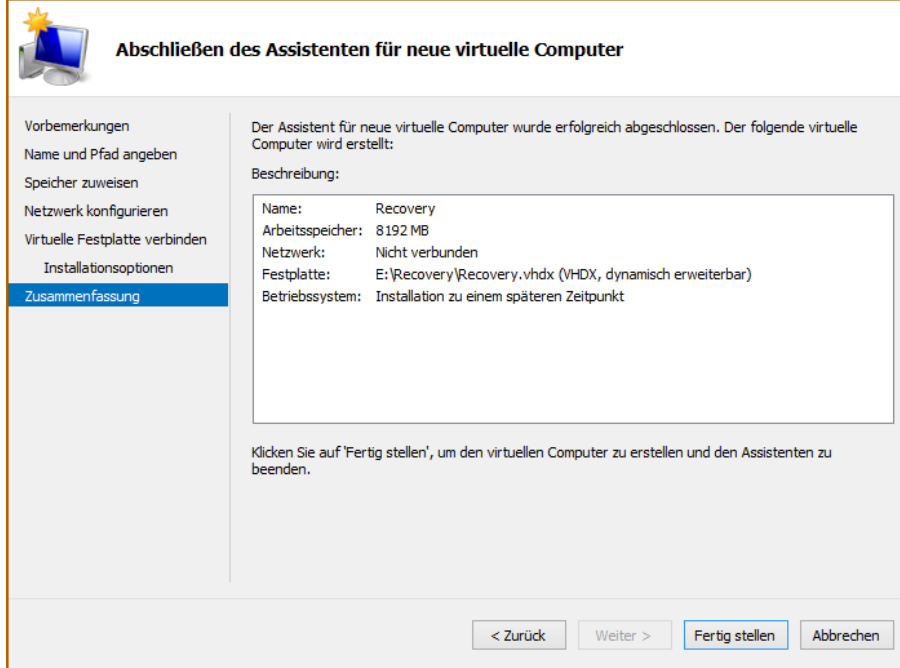
Medien  
Virtuelle Diskette (VFD): [Text] Durchsuchen...

Betriebssystem von einem netzwerkbasierten Installationsserver installieren

 Der Netzwerkkadappter ist nicht verbunden. Wechseln Sie für eine netzwerkbasierte Installation zur Netzwerkkonfigurationsseite, und stellen Sie eine Verbindung her.

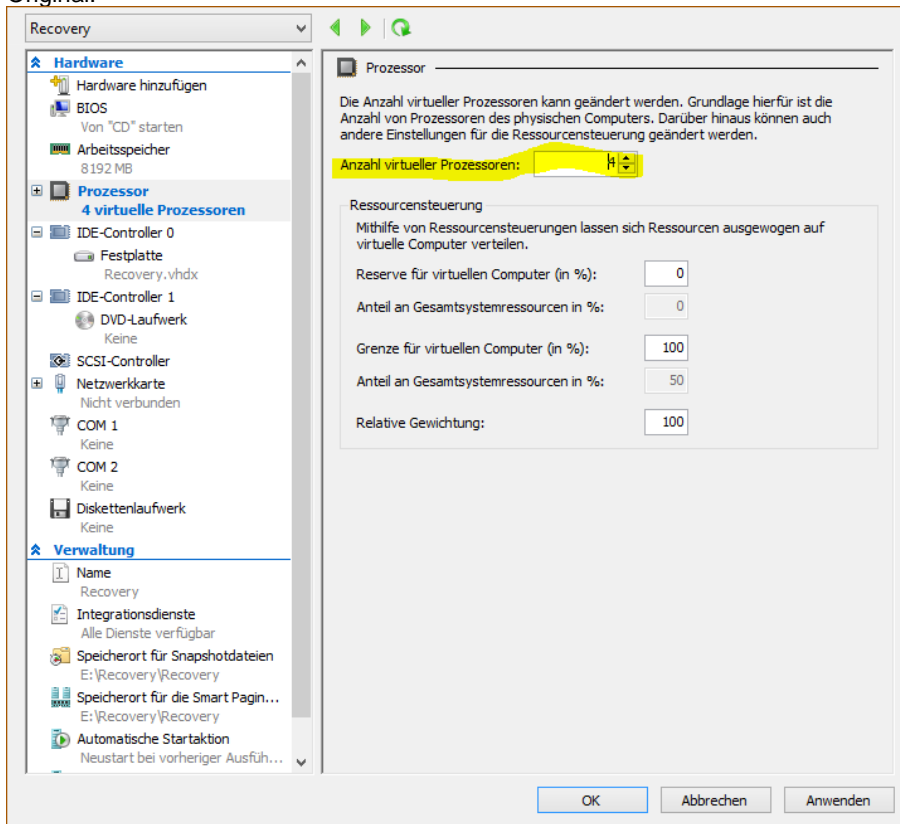
< Zurück Weiter > Fertig stellen Abbrechen

- Die Zusammenfassung der neuen VM.

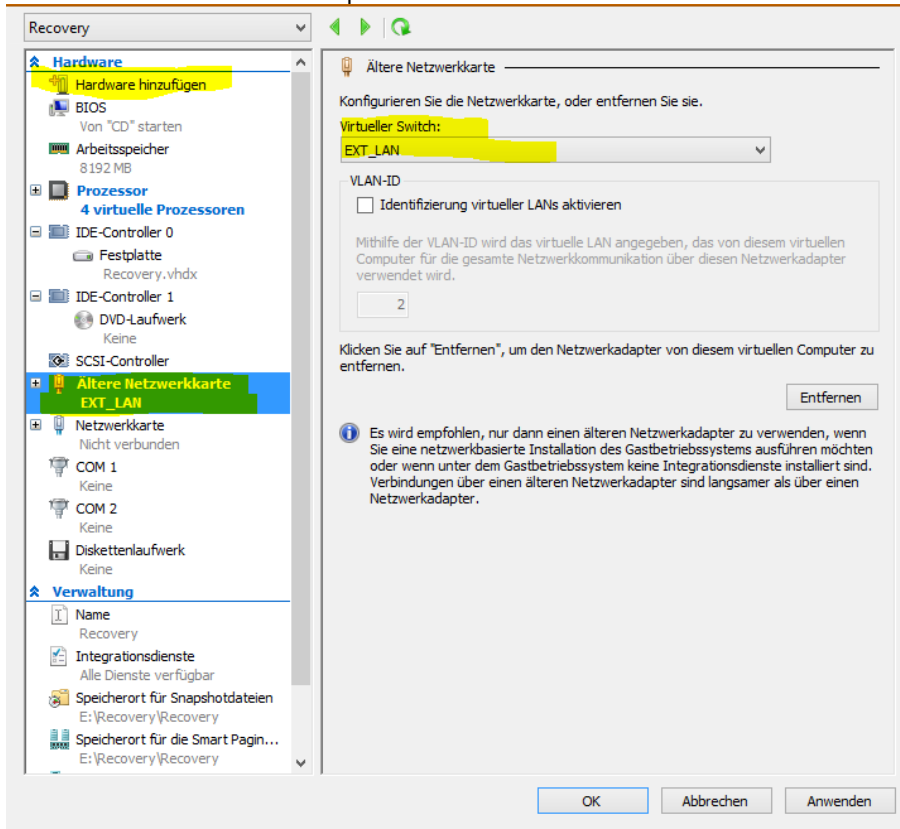


## b. Nachbearbeiten der virtuellen Maschine

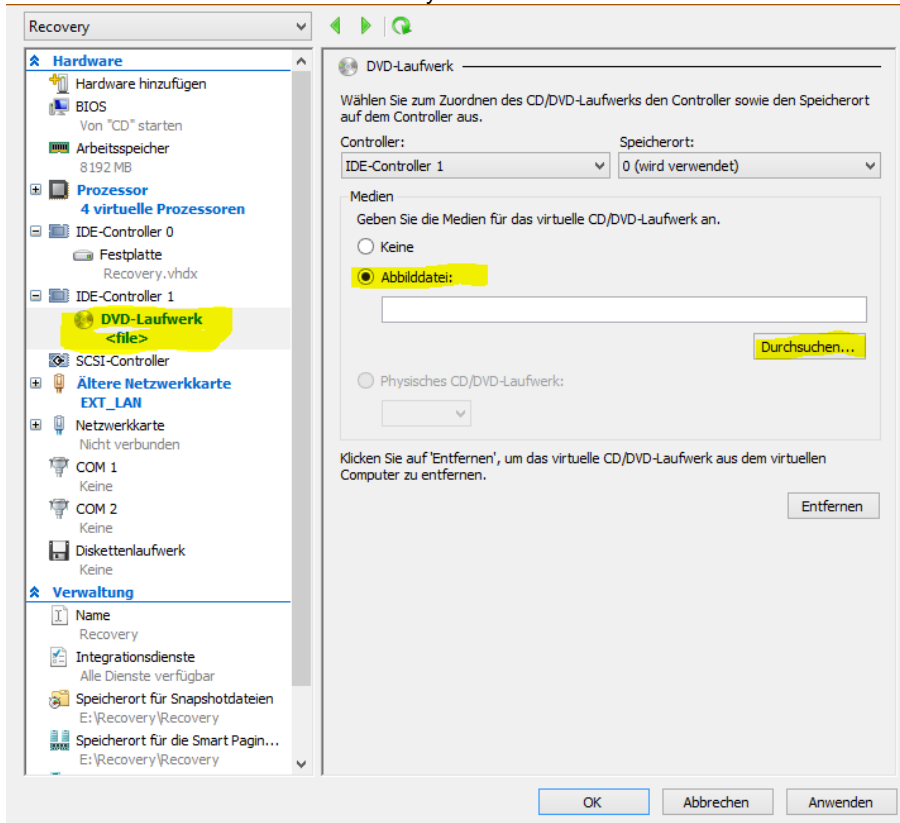
- Öffnen Sie die Eigenschaften, der eben erstellten VM. Verwenden Sie so viele CPU wie im Original.



- Fügen Sie eine neue Hardware hinzu (Ältere Netzwerkkarte) und verbinden Sie diese mit Ihrem Netzwerk. Im RecoveryModus versteht Windows 2008 die modernere Version leider nicht. Auf diese Art und Weise sparen wir uns umständliches hantieren mit Treibern.

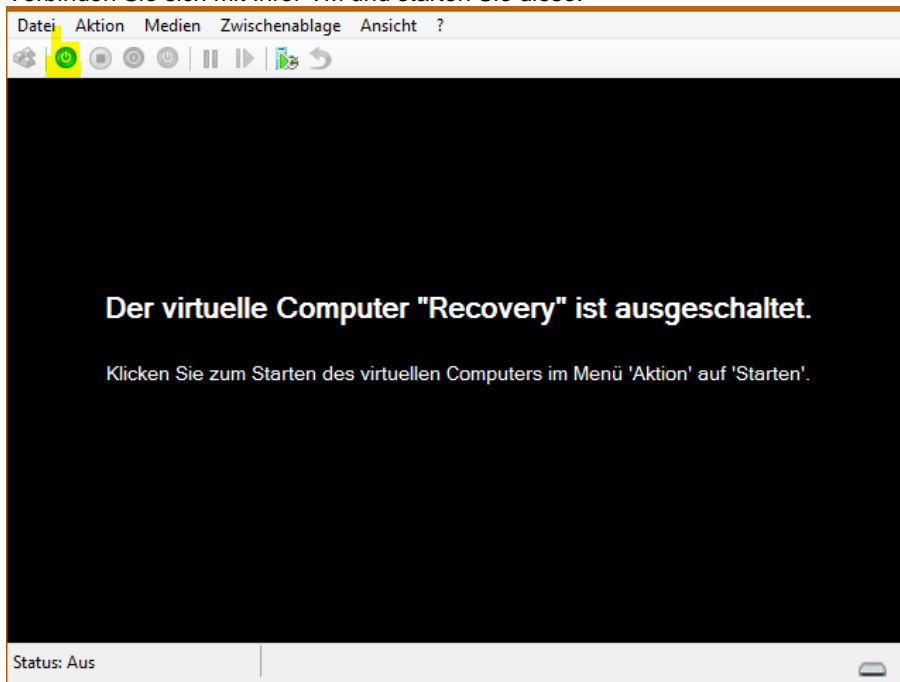


- Binden Sie die ISO-Datei des Betriebssystems ein und beenden Sie mit OK.

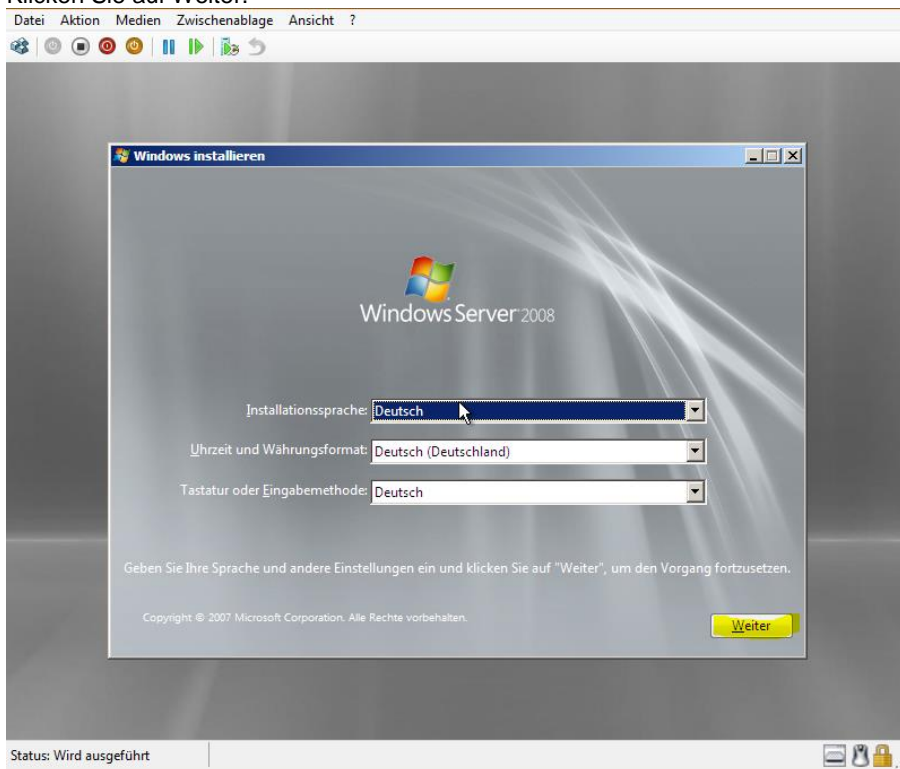


### c. Start der virtuellen Maschine

- Verbinden Sie sich mit Ihrer VM und starten Sie diese.

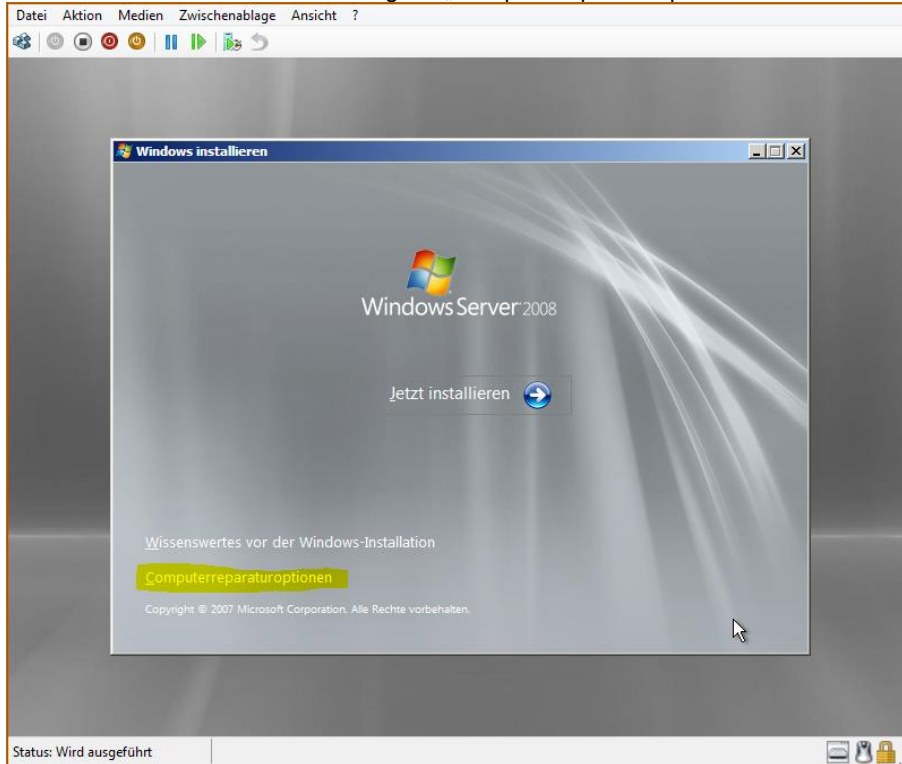


- Da wir eine leere Festplatte in dieser VM haben, bootet Windows automatisch vom ISO. Klicken Sie auf Weiter.

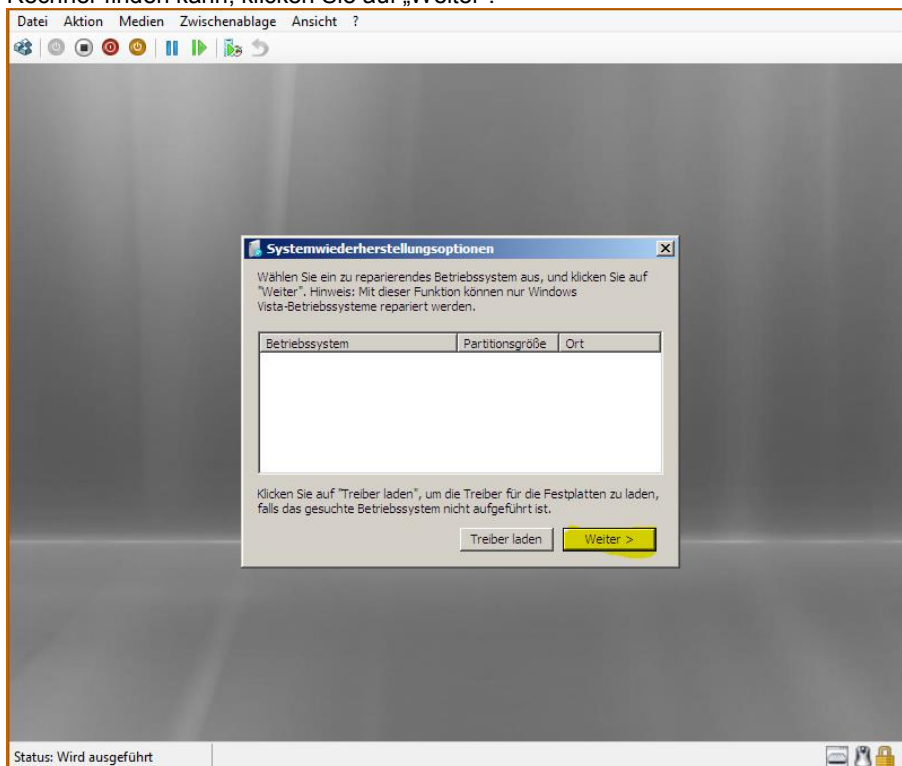




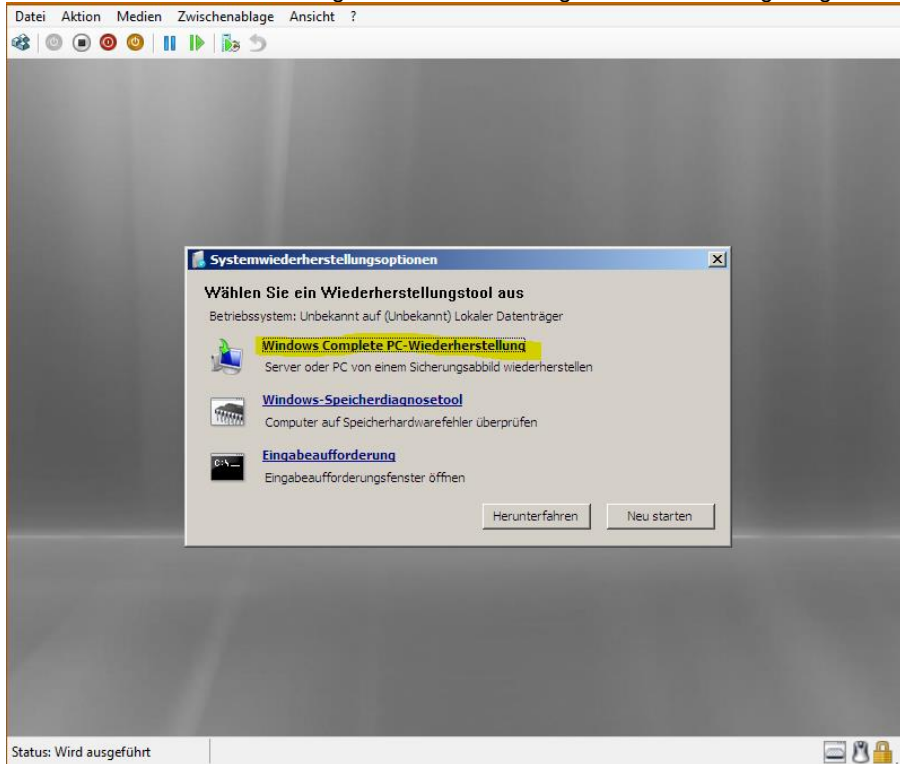
- Klicken Sie für die Wiederherstellung auf „Computerreparaturoptionen“.



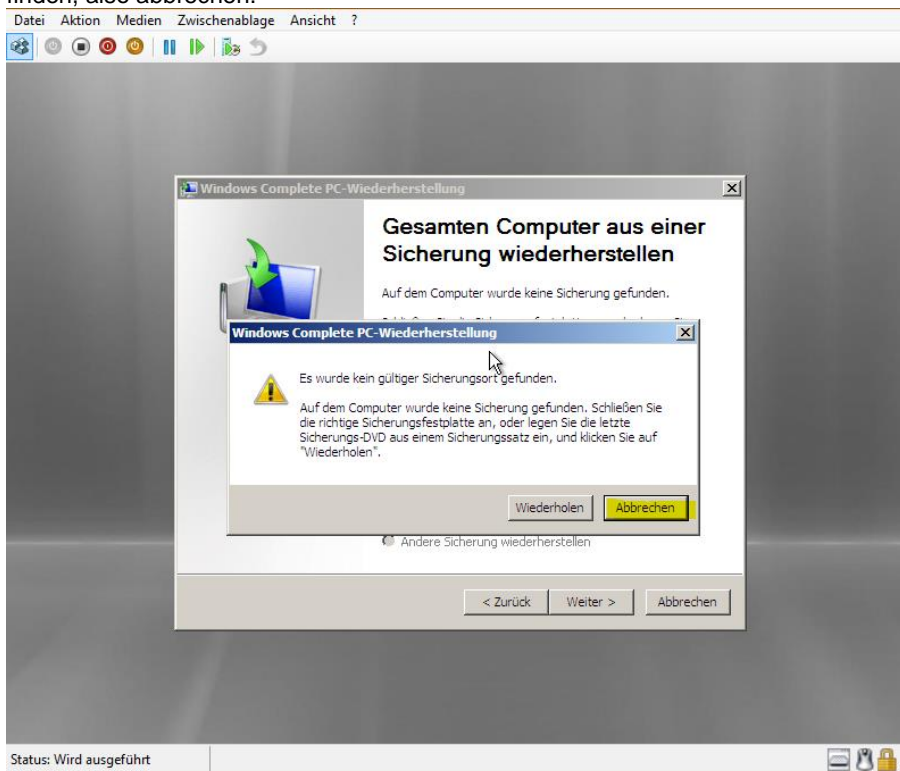
- Da der Wiederherstellungsmodus kein vorhandenes Betriebssystem auf einem leeren Rechner finden kann, klicken Sie auf „Weiter“.



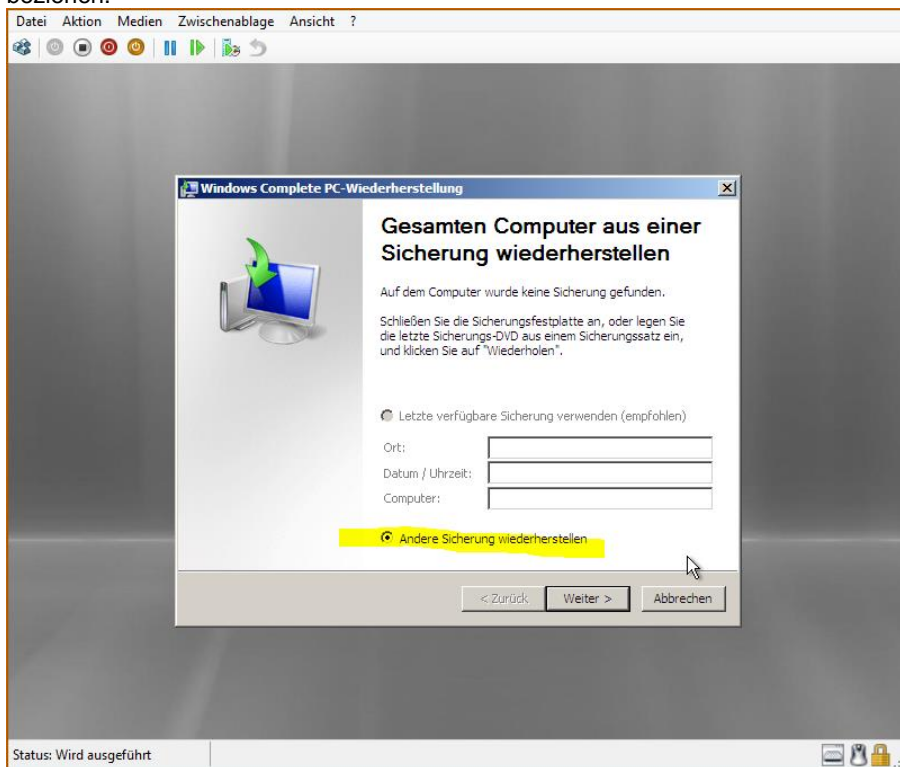
- Jetzt sind wir bei der vollständigen Wiederherstellung des Rechners angelangt.



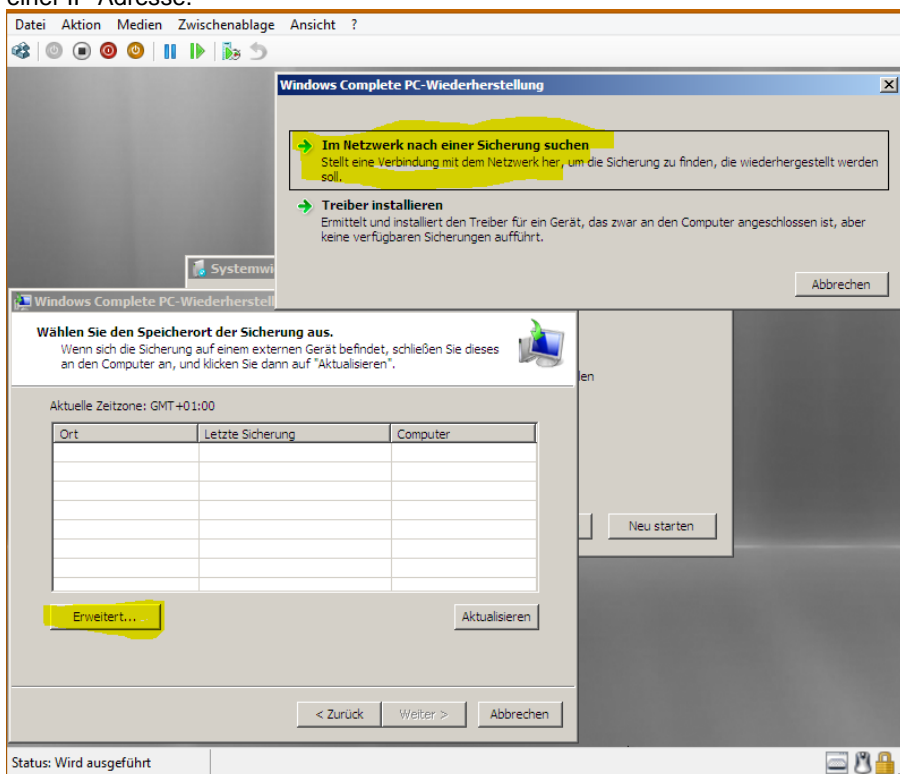
- Auf einem leeren Rechner wird die Wiederherstellung auch keine vorhandene Sicherung finden, also abbrechen.



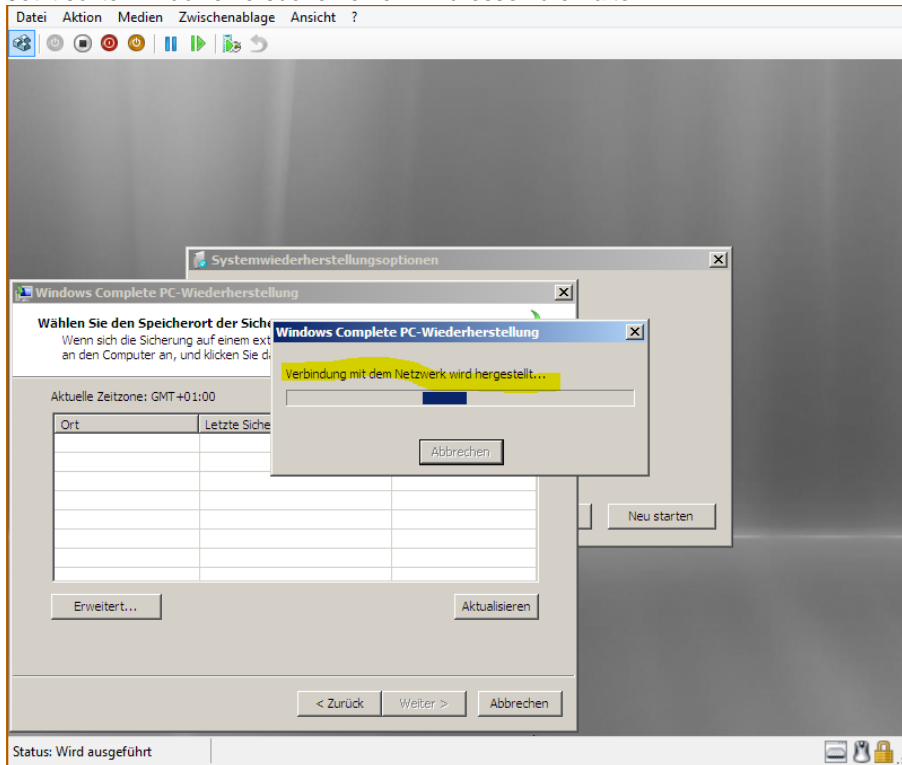
- Über den markierten Punkt können wir die Daten einer Sicherung aus dem Netzwerk beziehen.



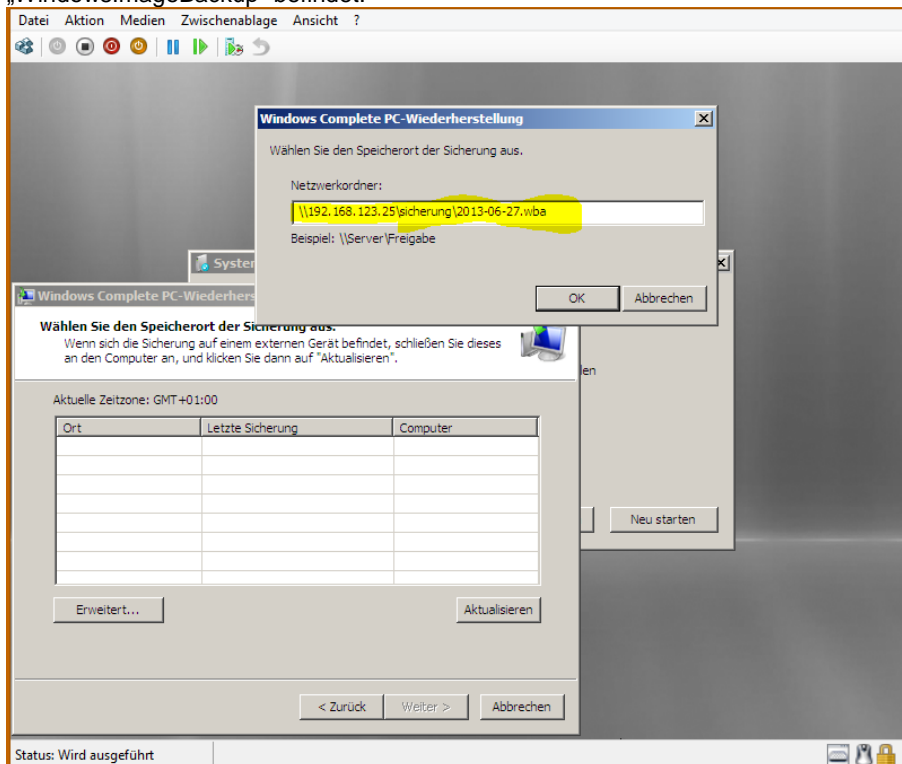
- Klicken Sie im Fenster (unten links) auf erweitert. Es öffnet sich der Netzwerkdialog (oben rechts) und wir sagen der Wiederherstellung, dass wir eine Sicherung im Netzwerk liegen haben. Bestätigen Sie die darauf folgende Meldung. Windows sucht jetzt, per DHCP, nach einer IP-Adresse.



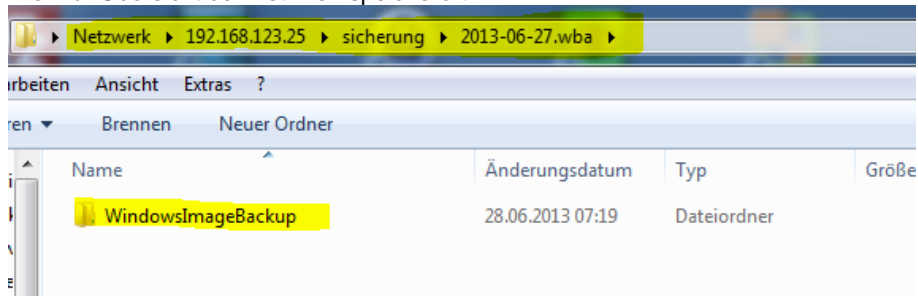
- Jetzt sollte Windows versuchen eine IP-Adresse zu erhalten



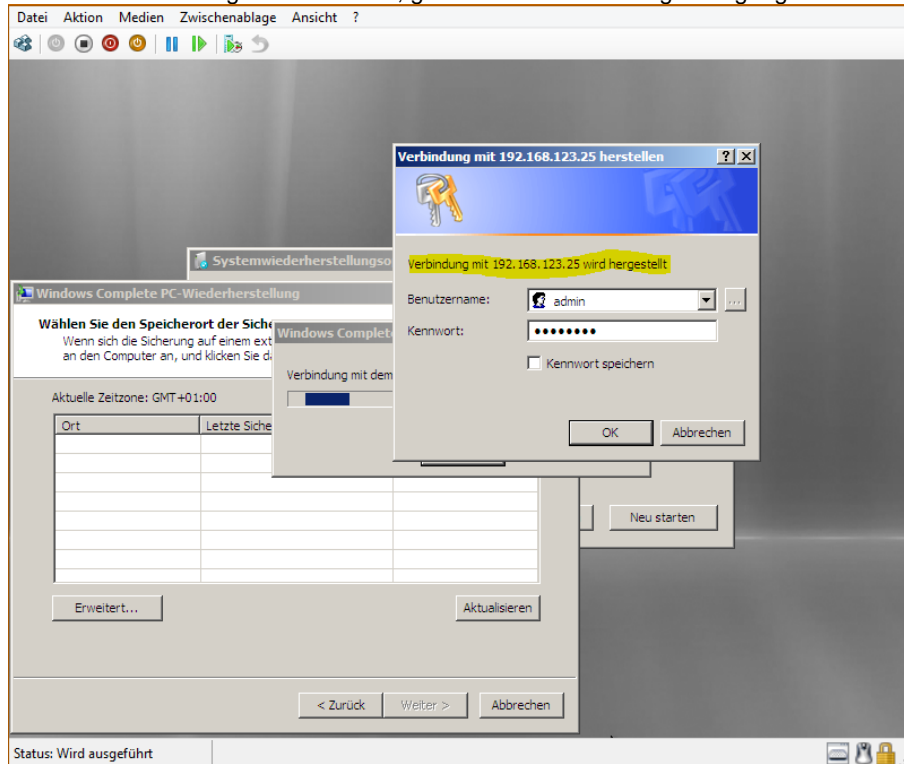
- Wenn Windows eine IP-Adresse erhalten hat, müssen Sie den Sicherungsort der vorhandenen Datensicherung angeben. Geben Sie den Ordner an, in dem sich der Ordner „WindowsImageBackup“ befindet.



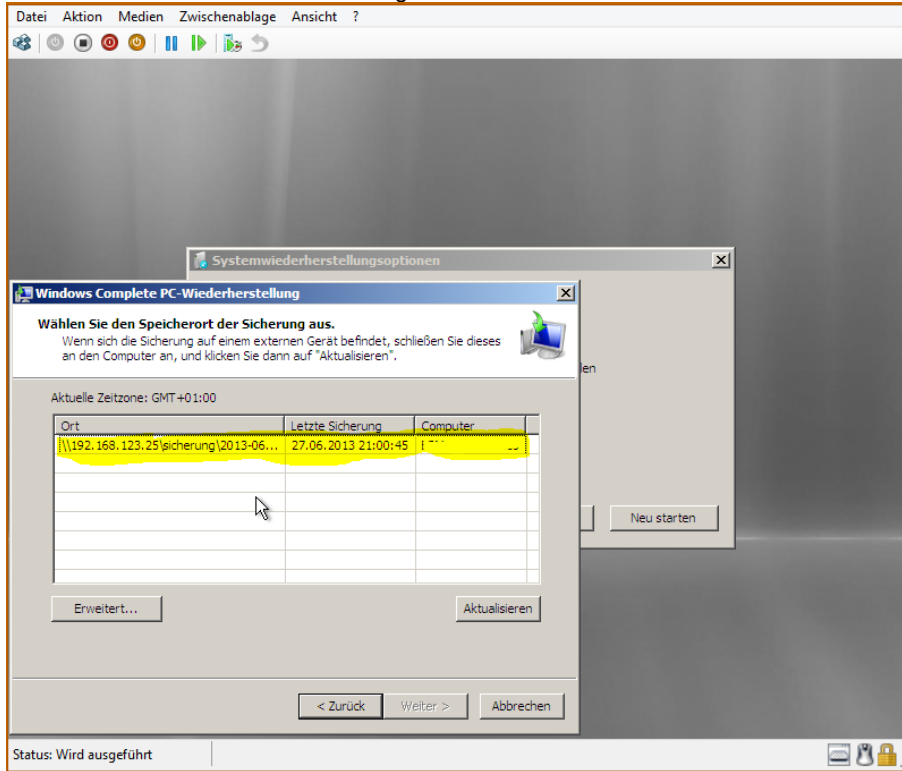
- Hier zur Übersicht der Netzwerkspeicherort



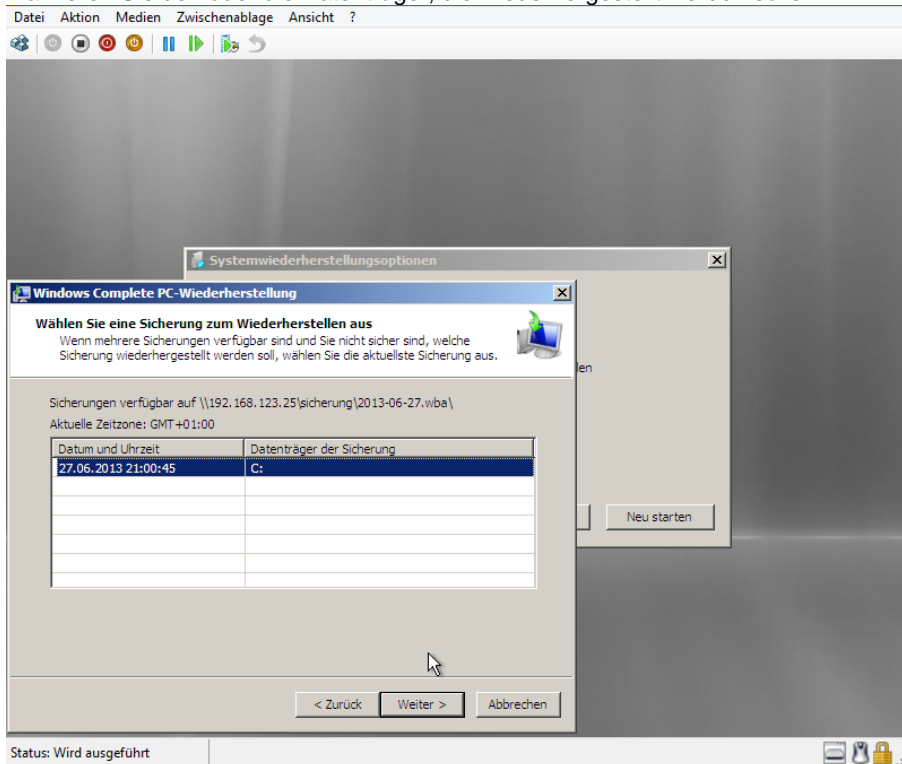
- Falls eine Anmeldung erforderlich ist, geben Sie die notwendigen Zugangsdaten an.



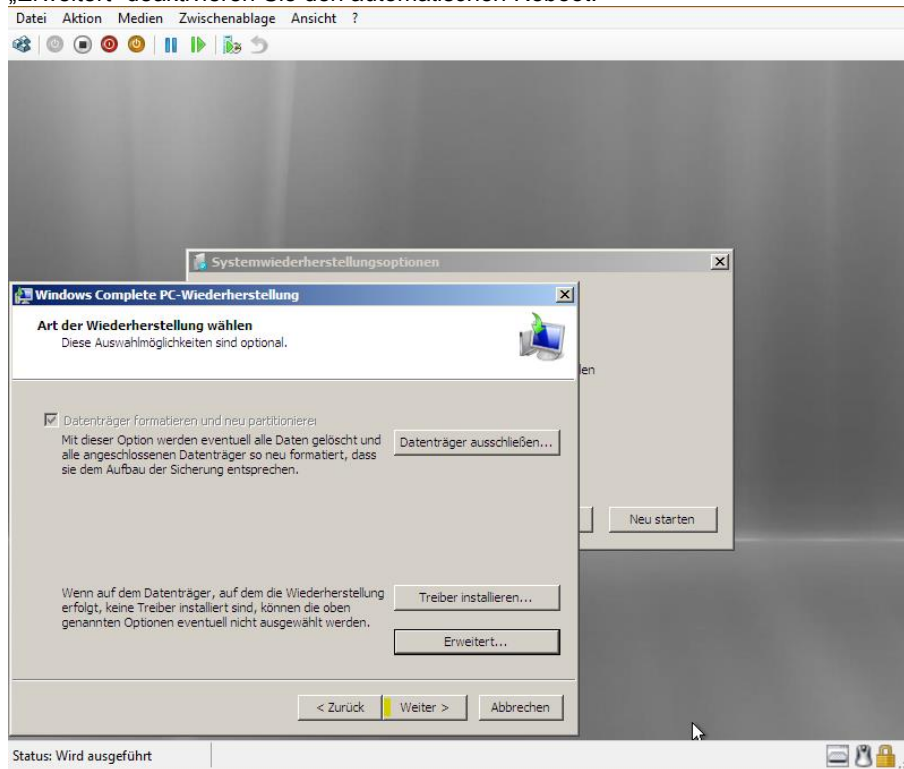
- Markieren Sie die erkannte Sicherung und klicken Sie auf weiter.



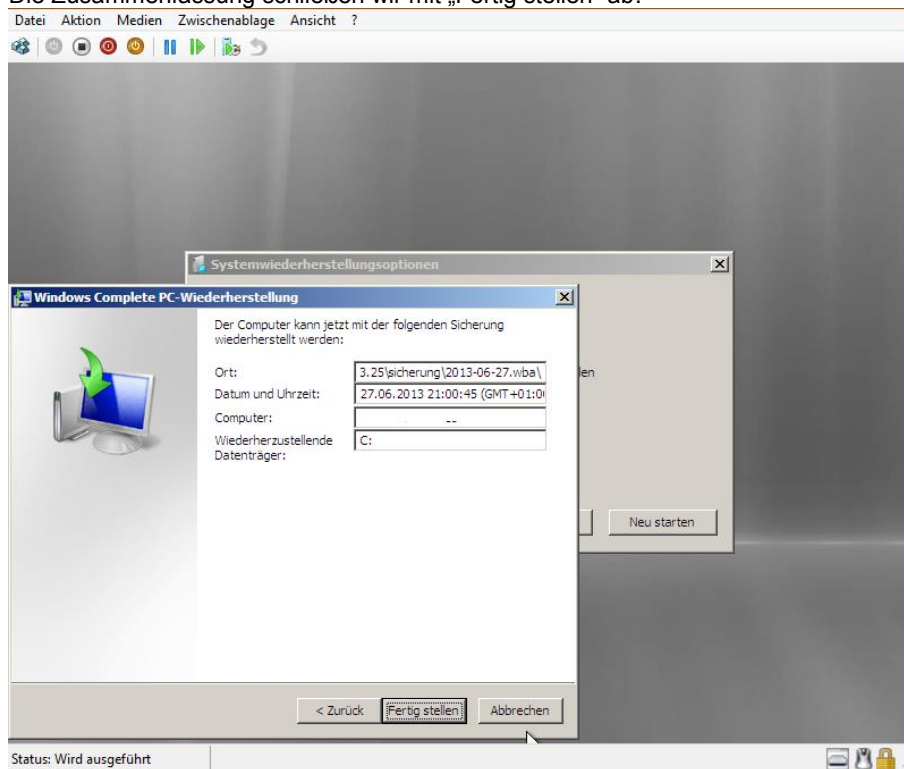
- Markieren Sie den oder die Datenträger, die wiederhergestellt werden sollen.



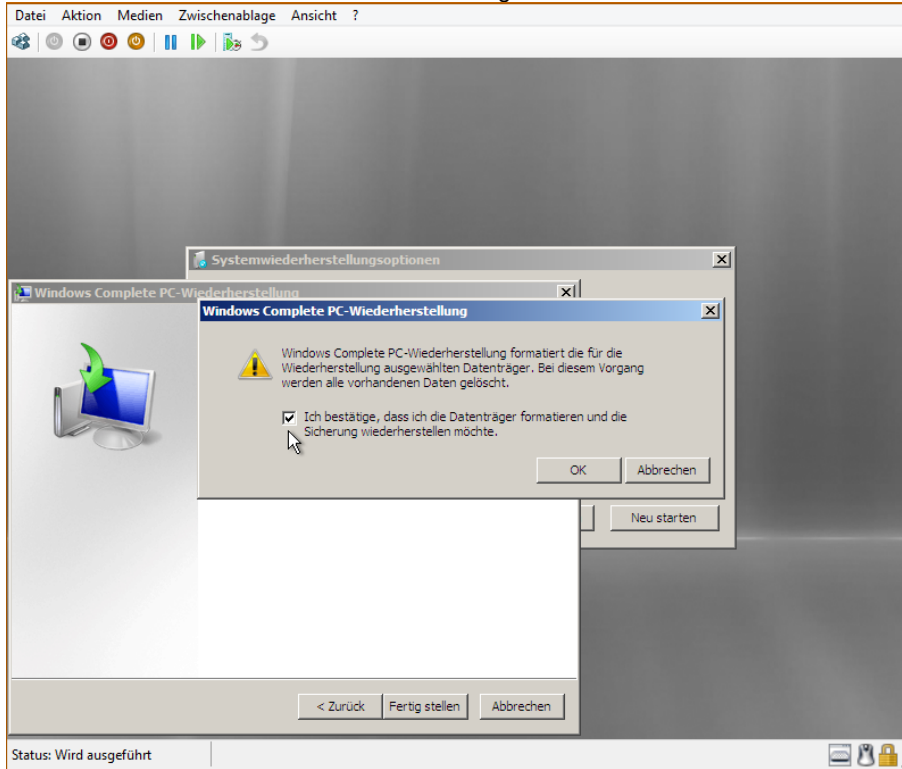
- Schauen Sie sich an, was sich hinter den 3 Schaltflächen verbirgt. Über die Schaltfläche „Erweitert“ deaktivieren Sie den automatischen Reboot.



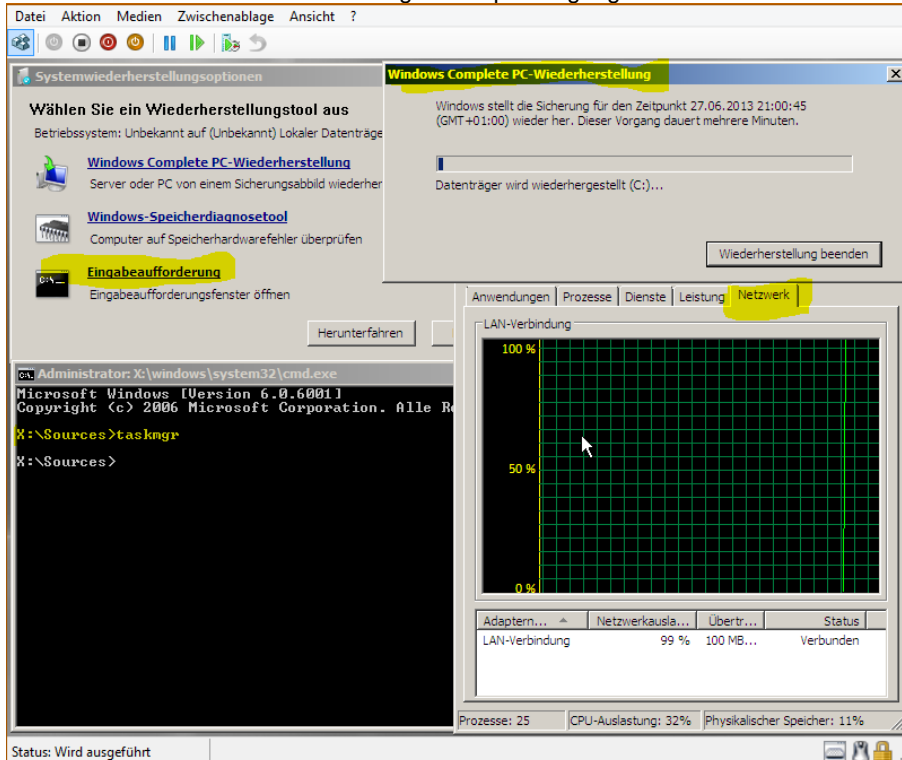
- Die Zusammenfassung schließen wir mit „Fertig stellen“ ab.



- Natürlich kommt zum Schluss noch eine Abfrage ob wir uns dessen sicher sind.

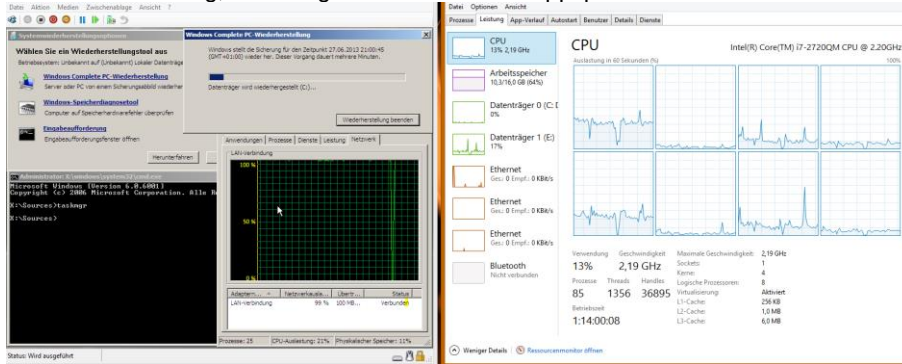


- Hier eine etwas erweiterte Darstellung des Kopiervorgangs





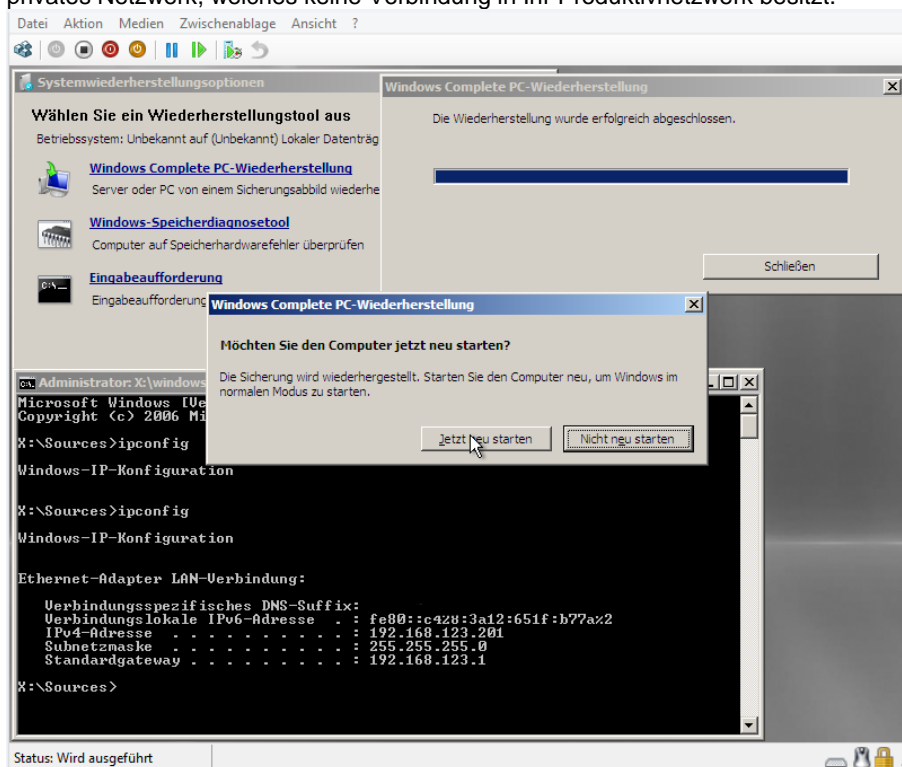
- Hier die Darstellung, was zeitgleich auf meinem Lappi passiert.



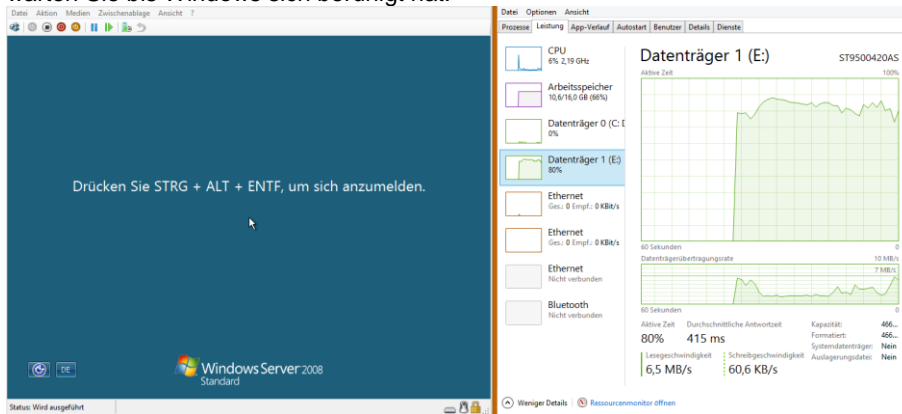
- Das passiert derzeit auf meiner Festplatte.  
Die Festplattendatei der VM wächst, als dyn. HDD, mit den kopierten Daten mit.

Name	Änderungsdatum	Typ	Größe
Recovery	28.06.2013 13:45	Dateiordner	
Recovery.vhdx	01.07.2013 09:04	Festplatten-Image...	37.031.936 KB
Win2k8_ger_x64.iso	08.12.2009 09:42	ISO Image	2.779.392 KB

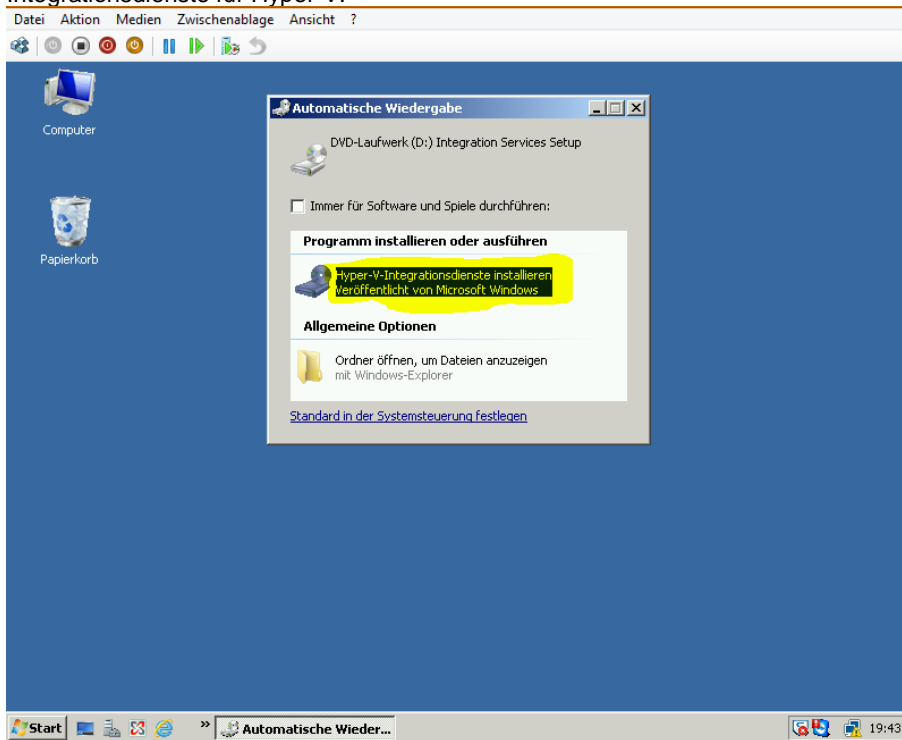
- **JETZT NICHT NEU STARTEN!**  
Falls Sie eine Testwiederherstellung durchführen wollen und das Originalsystem noch läuft, denken Sie bitte daran, dass Windows auch per Rundspruch kommuniziert. Das wiederhergestellte System darf sich jetzt auf keinen Fall im gleichen Netzwerk befinden wie das Original! Rekonfigurieren Sie im einfachsten Fall die virtuellen Netzwerkkarten auf ein privates Netzwerk, welches keine Verbindung in Ihr Produktivnetzwerk besitzt.



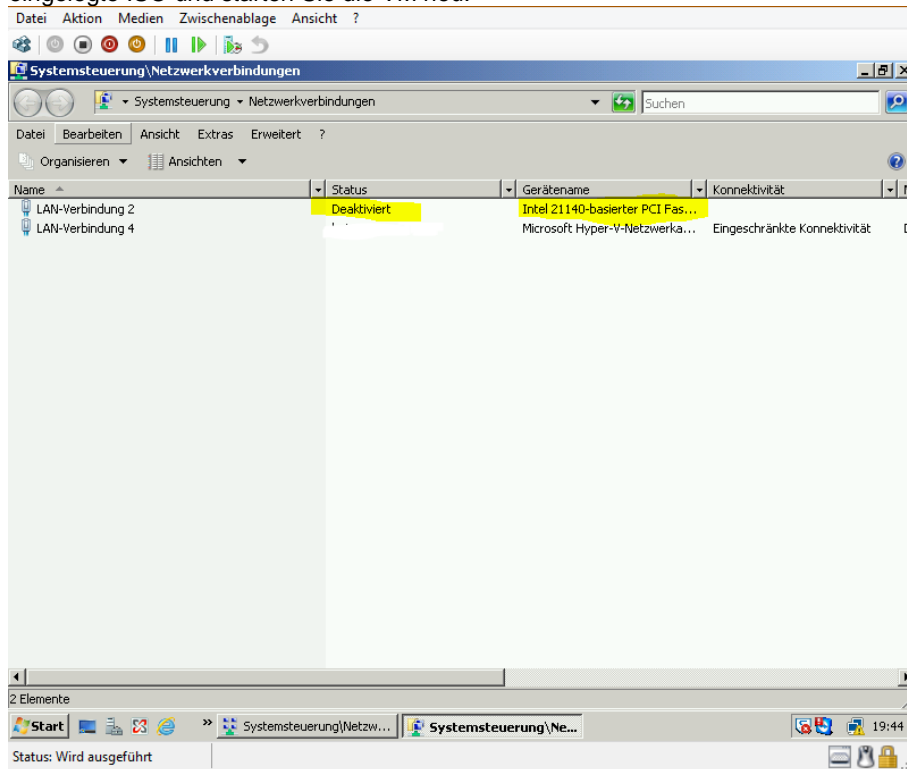
- Entfernen Sie das ISO aus der virtuellen Maschine (☺) und starten Sie die VM neu. Jetzt warten Sie bis Windows sich beruhigt hat.



- Nach erfolgreicher Anmeldung installieren Sie die aktuelle Version der Windows-Integrationsdienste für Hyper-V.



- Nach der Installation der Integrationsdienste deaktivieren Sie die „ältere Netzwerkkarte“ und vergeben an der anderen Netzwerkkarte eine feste IP-Adresse. Entfernen Sie das eingelegte ISO und starten Sie die VM neu.



- Jetzt müssen Sie nur noch warten, dieser Start kann ebenfalls etwas länger dauern. Wenn die, als VM, wiederhergestellte Datensicherung sauber läuft sollten Sie diese möglichst bald herunterfahren und eine Kopie davon anfertigen. Dies gilt natürlich nur für eine Wiederherstellung nach einem Ernstfall, wenn der eigentliche Server nicht mehr verfügbar ist. Bei einer Testwiederherstellung ist es jetzt Ihre Aufgabe, die aufgetretenen Fehler zu analysieren und zu dokumentieren.

## 4. BareMetalRecovery in einer physikalischen Umgebung

Die vollständige Wiederherstellung eines physikalischen Rechners unterscheidet sich zur virtuellen Umgebung dahingehend, dass Sie das Ziel der Wiederherstellung anfassen können.

## 5. Nacharbeiten

Nach der Wiederherstellung haben Sie noch folgende Aufgaben durchzuführen:

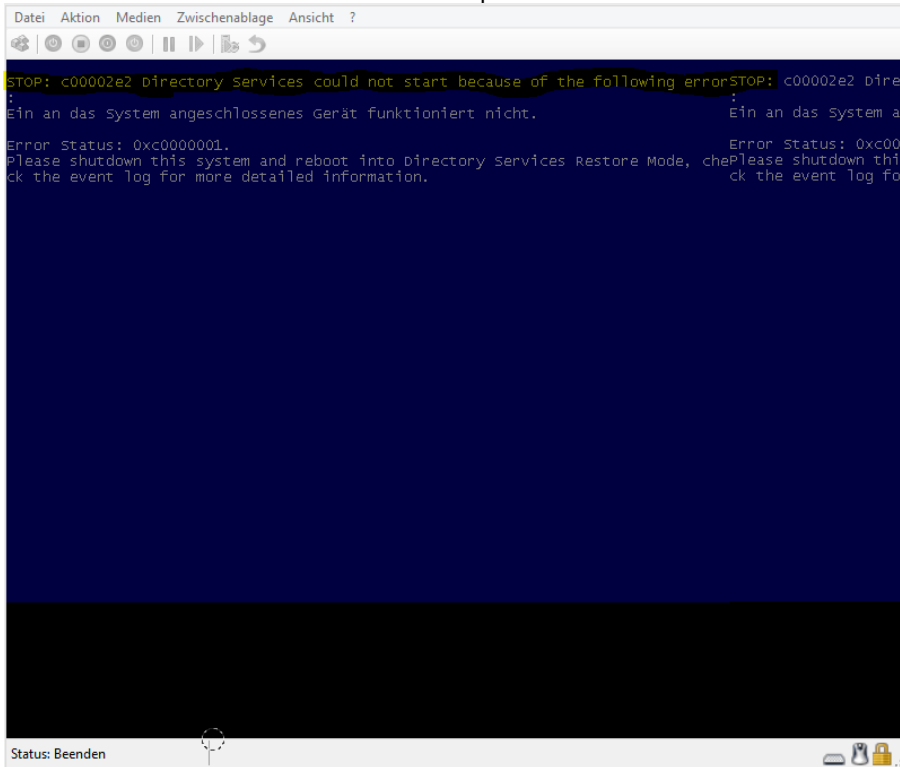
- Falls Sie Daten von diesem Rechner benötigen
  - a. Dateien können Sie ohne weiteres Kopieren
  - b. Bei Datenbanken benötigen Sie das Wissen und die notwendigen Ex- und Importwerkzeuge
  - c. Wenn es sich um den Exchange handelt:  
<http://www.msxfaq.de/tools/expublic/index.htm>  
<http://www.msxfaq.de/tools/msexch/index.htm>
- Falls Sie den kompletten Rechner wieder herstellen mussten
  - a. Passen Sie die Datensicherung an, evtl. ist ein Umbau der ehemaligen Sicherungsmethodik notwendig.
  - b. Falls die Wiederherstellung als VM weiterlaufen soll, verschieben Sie diese auf Ihren VM-Host. Falls diese Maschine wieder ein Blech werden soll, besorgen Sie Ersatz.
  - c. Lassen Sie den Rechner ein paar Tage laufen und bearbeiten Sie evtl. auftretende Probleme.
  - d. Sie sollten einige Tage ohne Produktaktivierung auskommen. Führen Sie die WPA durch, wenn Ihre Ersatzhardware da ist und Sie das Überbrückungssystem auf die neue Hardware migriert haben.

## 6. Anhang

### a. BSOD 1 – Fehler im Active Directory

Aus unerfindlichen Gründen sind Fehler in der Datenbank des Active Directory möglich.

- Wenn es sich bei dieser Installation um den Rechner eines KMU handelt, ist es mit Sicherheit der der einzige DC. Kritisch wird es, wenn hierauf auch noch ein Exchange- und/oder Datenbankservers läuft. Bestes Beispiel ist ein Small Business Server.



- Für die Reparatur des ADS folgt man dem Microsoft Technet.  
NTDSUTIL: <http://technet.microsoft.com/de-de/library/cc753343%28v=ws.10%29.aspx>  
ESEUTIL: <http://technet.microsoft.com/de-de/library/hh875546.aspx>
- Reparieren der Datenbank (hoffentlich)
  - Server im ADS-Restore-Modus starten und als Admin anmelden
  - Eine DOS-Box mit erhöhten Rechten öffnen
  - „ntdsutil“ eintippen und ENTER drücken
  - „activate instance NTDS“ eintippen und ENTER drücken
  - „files“ eintippen und ENTER drücken  
Jetzt sollten Sie erfahren, wo die Probleme liegen.
  - „quit“ eintippen und ENTER drücken
  - Führen Sie eine Sicherheitskopie Ihrer NTDS-Datenbank und der zugehörigen Logfiles durch. Das Standardverzeichnis lautet C:\Windows\ntds\.
  - Führen Sie eine Integritätskontrolle durch  
esentutl /g /Pfad/zur/ntds.dit
  - Führen Sie die Reparatur durch  
esentutl /p /Pfad/zur/ntds.dit
  - Führen Sie zur Kontrolle die Schritte a – e durch
  - Starten Sie den Server neu

## b. BSOD 2 – Inaccessible Boot Device

Dieser Fehler tritt meistens dann auf, wenn Sie die Wiederherstellung auf eine andere physische Hardware durchführen. In den häufigsten Fällen ist ein anderer Festplattencontroller die Ursache.

- Auf diese Weise teilt Ihnen Windows mit, dass es Probleme mit dem Datenträger hat.

```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

INACCESSIBLE_BOOT_DEVICE

If this is the first time you've seen this error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:
*** STOP: 0x0000007B (0xF741B84C, 0xC0000034, 0x00000000, 0x00000000)

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

- Suchen Sie nach MERGEIDE von [www.andysblog.de](http://www.andysblog.de). Die erweiterte Registry-Datei ist ein guter Anlaufpunkt zur Reparatur.

<http://www.andysblog.de/windows-mergeide-ist-nicht-gleich-mergeide>