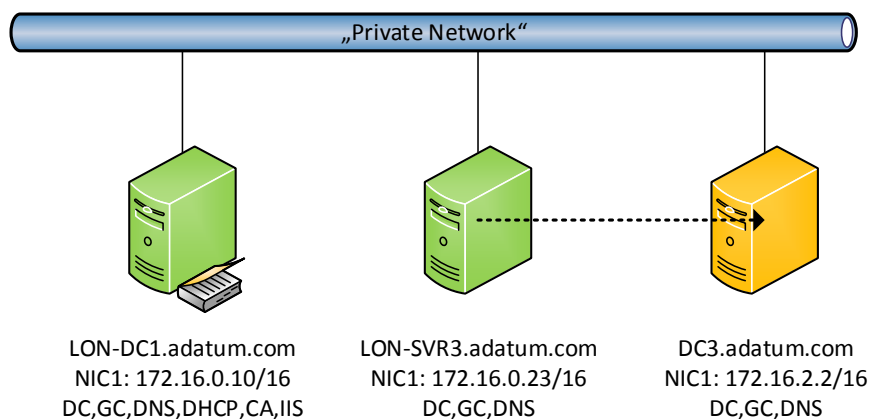


Inhalt

1.	Szenario.....	1
2.	Voraussetzungen	1
	auf der Klon-Vorlage LON-SVR3	1
	in der Domäne	1
	Hyper-Visor	1
3.	Arbeitsschritte:.....	2
	Erstellen der Klonvorlage	2
	im Hyper-Visor.....	4
4.	Der Klon-Vorgang.....	4
	Prüfung im AD.....	5

1. Szenario

- LON-DC1 stellt allein adatum.com bereit, LON-SVR3 wird der 2. DC und anschließend eine Klon-Vorlage für DC3:



2. Voraussetzungen

auf der Klon-Vorlage LON-SVR3

- Es dürfen keine weiteren Rollen als ADDS und DNS installiert sein
- Es dürfen keine sonstigen Anwendungen installiert sein
- Der DC darf keine FSMO ausführen
- Die VM des DCs darf keinen SnapShot haben

in der Domäne

- es wird ein PDC mit Windows Server 2012 oder höher benötigt
- das Computerkonto der Klonvorlage muss in der Gruppe „Cloneable Domain Controllers“ Mitglied sein

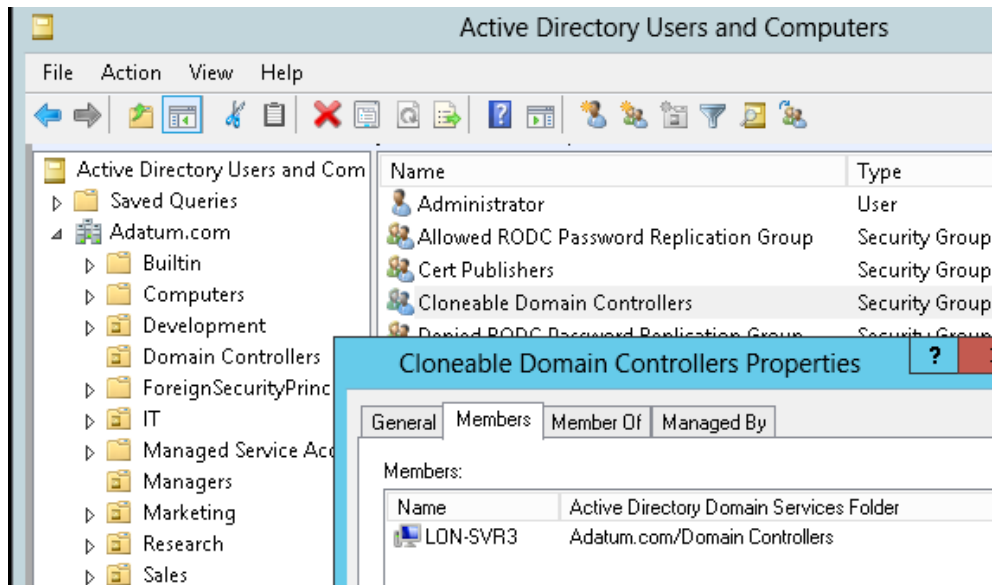
Hyper-Visor

- der Hyper-Visor muss das Feature VM-GenerationID unterstützen

3. Arbeitsschritte:

Erstellen der Klonvorlage

- Installiere ADDS und DNS auf LON-SVR3
- Nehme LON-SVR3 in die Gruppe „Klonbare-DCs“ auf:



- Erstelle die Konfigurations-xml-Dateien: (Ausführung in Powershell [Bild2])

```
# Beispielscript
# listet alle nicht kompatiblen Dienste:
Get-ADDCCloningExcludedApplicationList

# nimmt diese Dienste in die Ausnahmedatei auf:
Get-ADDCCloningExcludedApplicationList -GenerateXml
cls

#del C:\windows\NTDS\DCCloneConfig.xml

# erstellt die Config-Datei:
New-ADDCCloneConfigFile
-Static
-IPv4Address '172.16.2.2' `
-IPv4SubnetMask '255.255.0.0' `
-IPv4DefaultGateway '172.16.0.1' `
-IPv4DNSResolver '172.16.0.10' `
-SiteName 'Muenchen'
-CloneComputerName 'DC1'
```

```

PS C:\> Get-ADDCCloningExcludedApplicationList -GenerateXml
The inclusion list was written to 'C:\Windows\NTDS\CustomDCCloneAllowList.xml'.
PS C:\> New-ADDCCloneConfigFile -CloneComputerName 'dc2' -IPv4Address '172.16.2.1' -IPv4DNSResolver '127.0.0.1' -IPv4SubnetMask '255.255.0.0' -Static
Running in 'Local' mode.
Starting PDC test: Verifying that the domain controller hosting the PDC FSMO role is running Windows Server 2012 or later...
Passed: The domain controller hosting the PDC FSMO role (LON-DC1.Adatum.com) was located and running Windows Server 2012 or later.

Verifying authorization: Checking if this domain controller is a member of the 'Cloneable Domain Controllers' group...
Located the local domain controller: (LON-SVR3.Adatum.com).
Querying the 'Cloneable Domain Controllers' group...
Pass: The local domain controller is a member of the 'Cloneable Domain Controllers' group.

Starting test: Validating the cloning allow list.
NOTE: C:\Windows\NTDS\CustomDCCloneAllowList.xml is being used as the defined inclusion list.
No excluded applications were detected.
Pass: No excluded applications were detected.

No valid clone configuration files were found at any of the supported locations.

All preliminary validation checks passed.

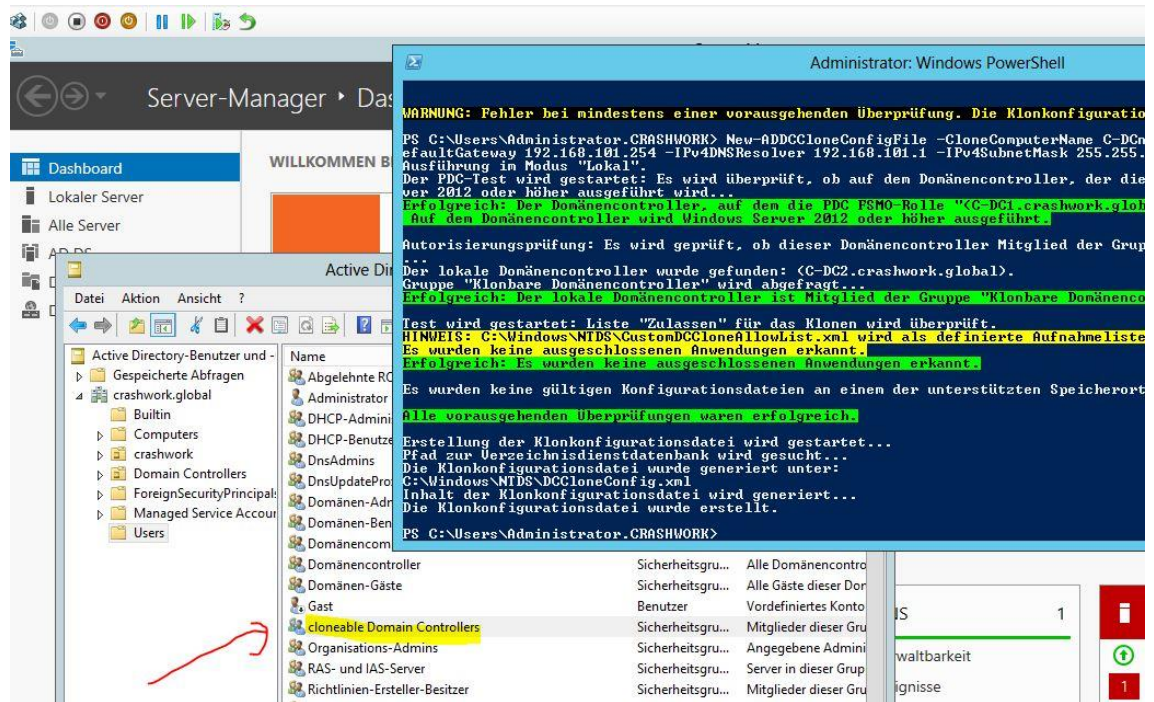
Starting creation of the clone configuration file...
Finding the path to the Directory Service database...
The clone configuration file was generated at:
C:\Windows\NTDS\DCCloneConfig.xml
Generating the clone configuration file content...
The clone configuration file has been created.

PS C:\>
    
```

- Achtung: der PowerShell-Befehl prüft die Gruppenmitgliedschaft. Hier gibt es einen Bug im Active Directory, wenn dieses unter einem DC erstellt oder auf Windows Server 2012 erweitert wurden und dieser DC eine deutsche Systemsprache verwendet:
 - Das Problem: Der Befehl findet die Gruppe nicht

The screenshot shows a Windows Server 2012 environment. In the background, the Server Manager console displays the Active Directory structure. The 'Klonbare Domänencontroller' group is highlighted in yellow. In the foreground, a PowerShell console window shows the execution of the 'New-ADDCCloneConfigFile' command. The output includes several error messages in German, such as 'Warnung: Die Gruppe "Klonbare Domänencontroller" kann nicht abgefragt werden.' and 'Hinweis: C:\Windows\NTDS\CustomDCCloneAllowList.xml wird als definierte Aufnahme...'. A red arrow points from the PowerShell window to the 'Klonbare Domänencontroller' group in the Server Manager console.

- Die Lösung: Die Gruppe muss umbenannt werden!



- Der Befehl erzeugt unter C:\Windows\NTDS die CloneConfig.xml-Datei:

```
<?xml version="1.0"?>
<d3c:DCCloneConfig xmlns:d3c="uri:microsoft.com:schemas:DCCloneConfig">
  <ComputerName>dc3</ComputerName>
  <IPSettings>
    <IPv4Settings>
      <StaticSettings>
        <Address>172.16.2.2</Address>
        <SubnetMask>255.255.0.0</SubnetMask>
        <DNSResolver>172.16.0.10</DNSResolver>
      </StaticSettings>
    </IPv4Settings>
  </IPSettings>
</d3c:DCCloneConfig>
```

Diese kann also auch danach offline über das Mounten der VHD des Klones editiert werden

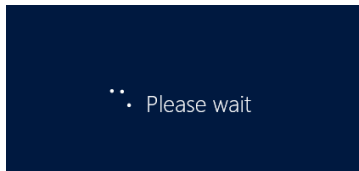
- Schalte LON-SVR3 aus

im Hyper-Visor

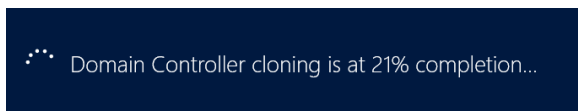
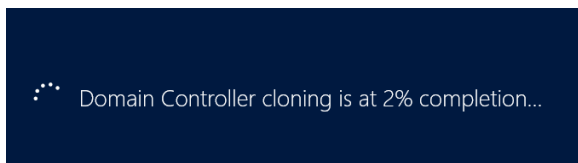
- Exportiere VM
- Importiere VM (als Kopie)

4. Der Klon-Vorgang

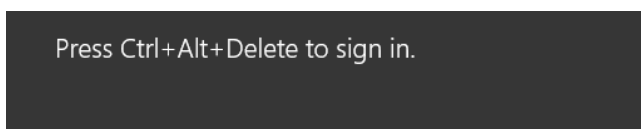
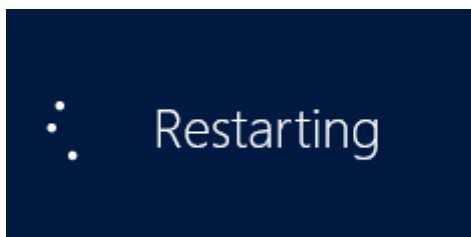
- starte die VM des Klones:



- Der DC prüft jetzt, ob seine VM-GenerationID, die er vom Hyper-Visor über die virtuelle BIOS erhält, mit seiner letzten ID übereinstimmt -> Da die VM-Kopie eine neue ID bekommen hat sind die letzte und die aktuelle ID unterschiedlich
 - Das Betriebssystem sucht nach der Clone-Config-Datei
 - Nun wird der PDC kontaktiert, um zu prüfen, ob die Konfiguration vielleicht schon einmal verwendet wurde und um zu prüfen, ob das alte Computerkonto in der Gruppe der klonbaren DCs enthalten ist
 - Jede Abweichung wird zu einem BlueScreen oder einem Start im Modus „Verzeichnisdienstwiederherstellung“ führen
- Für diese VM ist alles OK, daher wird das Cloning gestartet:

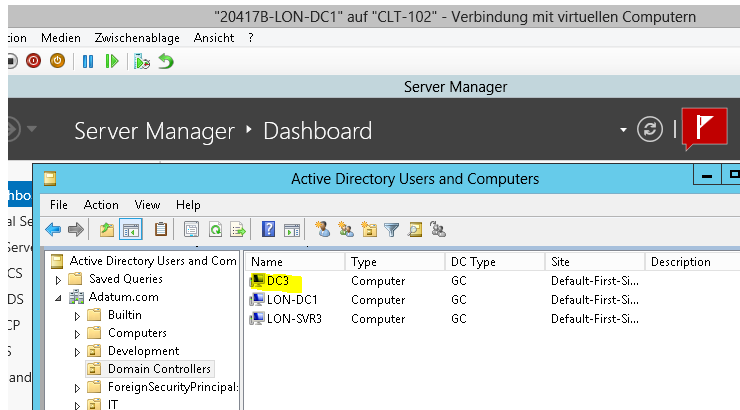


- Ein automatischer Neustart nach dem „Sysprep light“ startet den „neuen“ DC:

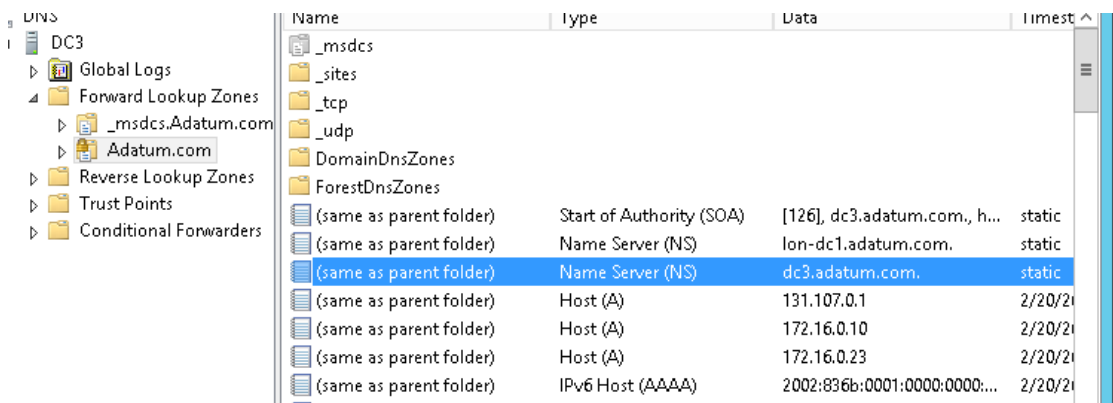


Prüfung im AD

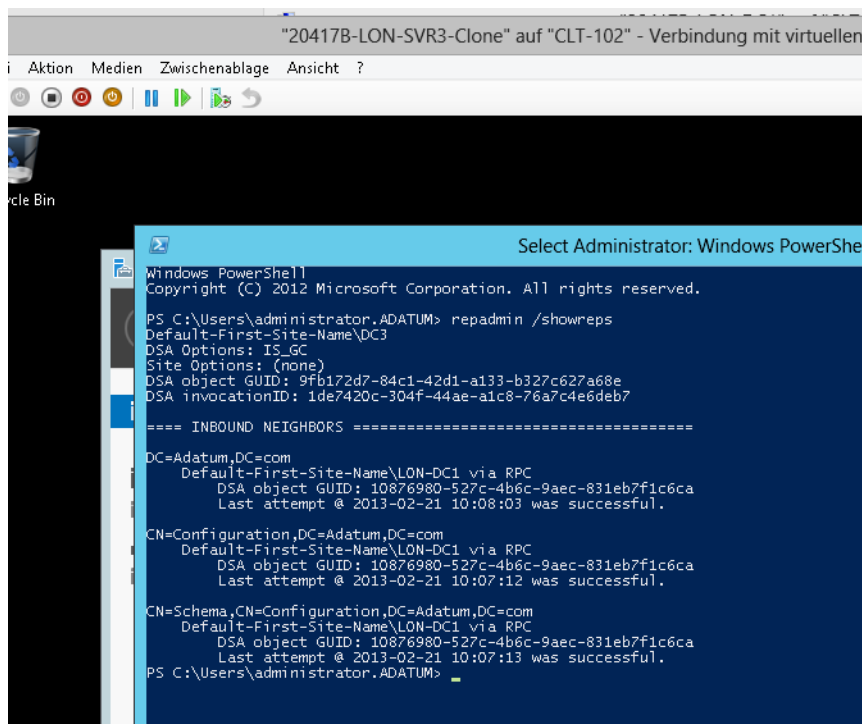
- unter den DCs sollte das neue Computerkonto gelistet werden:



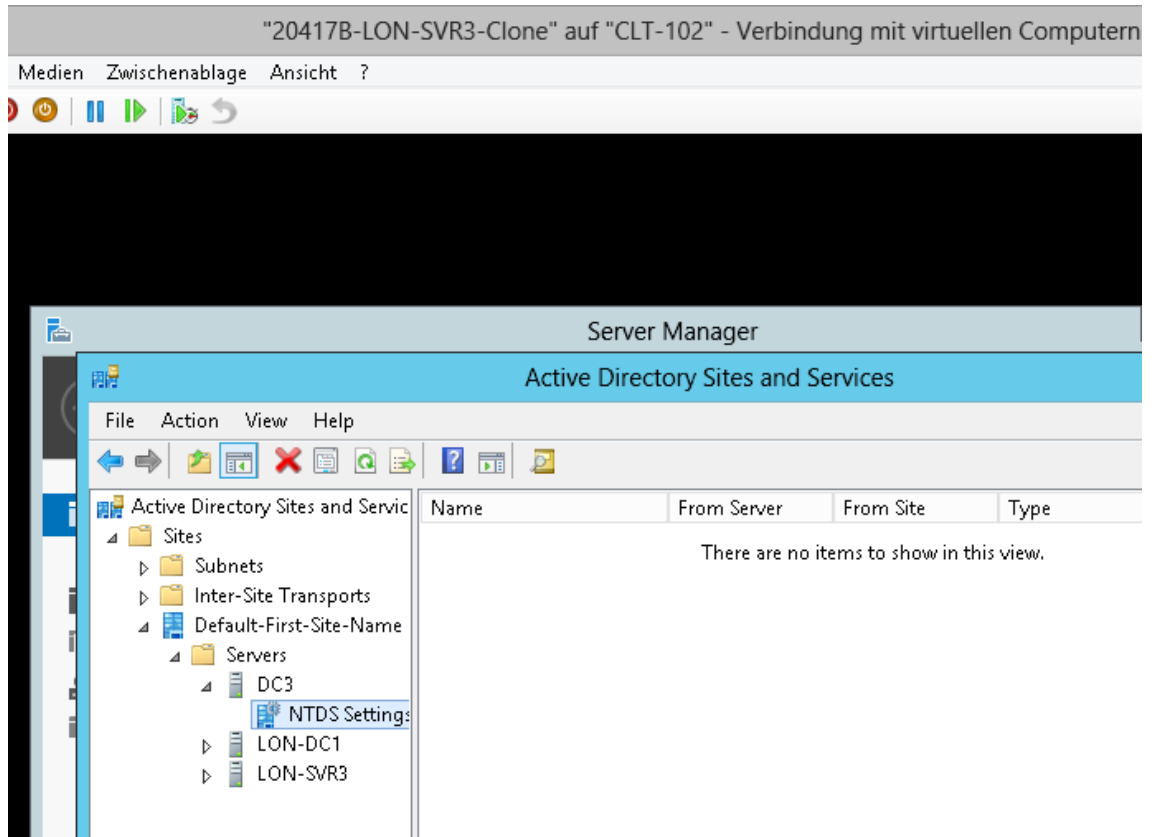
- im DNS sollte sich der neue DNS-Server als NS eintragen:



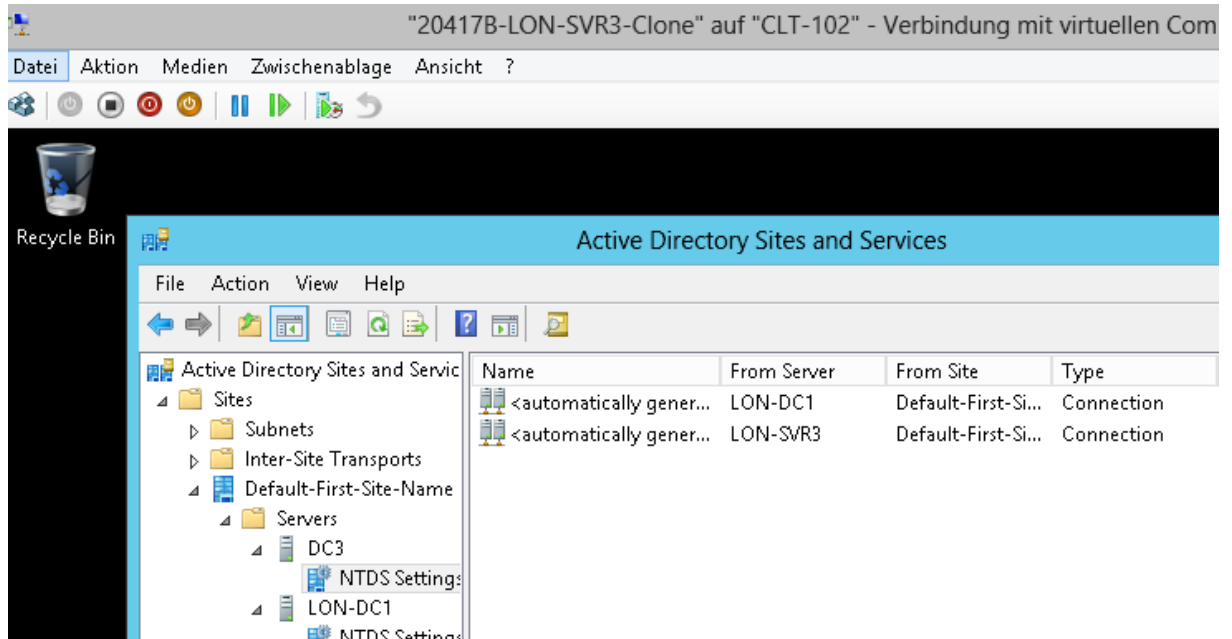
- Prüfung der Replikation: hier wird das gleiche Verhalten wie nach einen Standard-Deployment eines zusätzlichen DCs gefunden
 - der neue DC hat noch nicht alle Replikationsverbindungen eingetragen:



- Unter Sites-and-Services fehlen die ausgehandelten Replikationsverbindungen:



- Nach der Aushandlung über KCC sind diese nun vorhanden:



- und die Replikation wird ausgeführt:

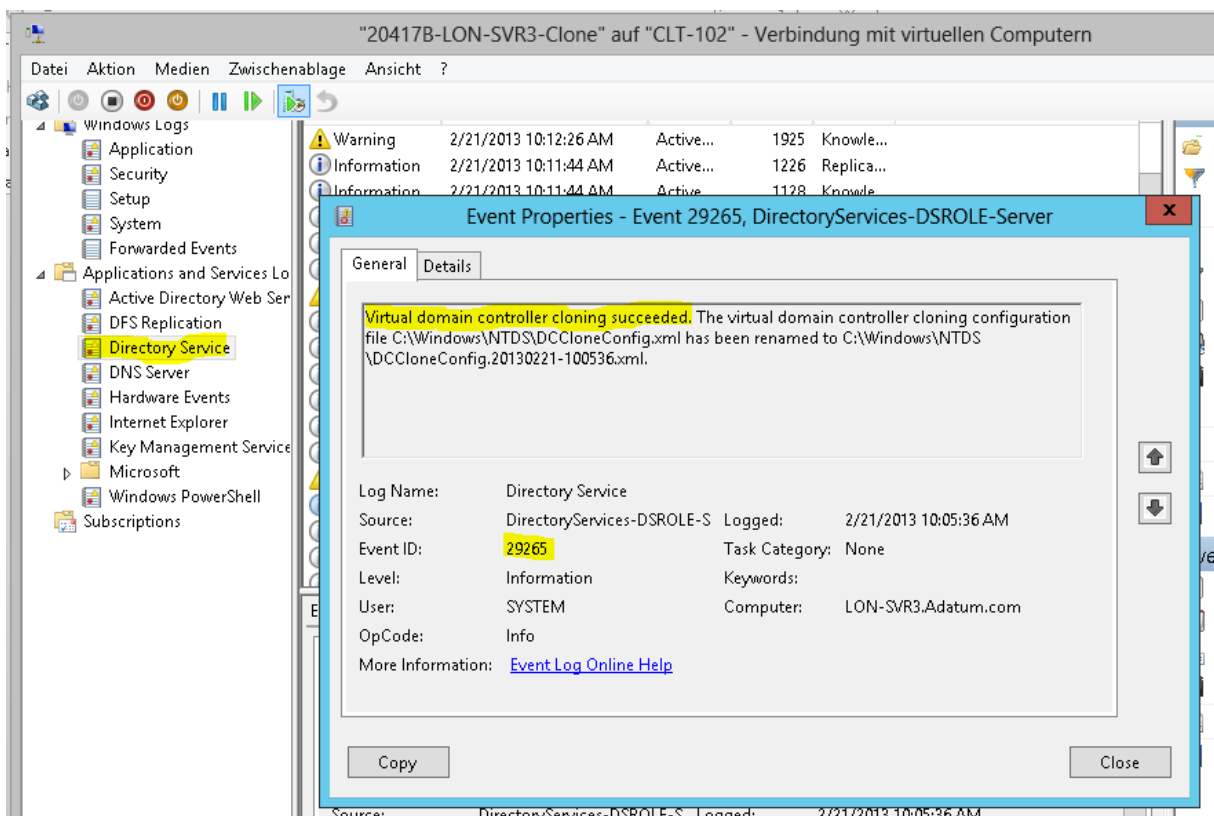
```

"20417B-LON-SVR3-Clone" auf "CLT-102" - Verbindung mit
n Zwischenablage Ansicht ?

Administrator: Windows Po
PS C:\Users\administrator.ADATUM> repadmin /showreps
Default-First-Site-Name\DC3
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: 9Fb172d7-84c1-42d1-a133-b327c627a68e
DSA invocationID: 1de7420c-304f-44ae-a1c8-76a7c4e6deb7

==== INBOUND NEIGHBORS =====
DC=Adatum,DC=com
  Default-First-Site-Name\LON-DC1 via RPC
  DSA object GUID: 10876980-527c-4b6c-9aec-831eb7f1c6ca
  Last attempt @ 2013-02-21 10:17:45 was successful.
CN=Configuration,DC=Adatum,DC=com
  Default-First-Site-Name\LON-DC1 via RPC
  DSA object GUID: 10876980-527c-4b6c-9aec-831eb7f1c6ca
  Last attempt @ 2013-02-21 10:16:07 was successful.
CN=Schema,CN=Configuration,DC=Adatum,DC=com
  Default-First-Site-Name\LON-DC1 via RPC
  DSA object GUID: 10876980-527c-4b6c-9aec-831eb7f1c6ca
  Last attempt @ 2013-02-21 10:07:13 was successful.
DC=DomainDnsZones,DC=Adatum,DC=com
  Default-First-Site-Name\LON-DC1 via RPC
  DSA object GUID: 10876980-527c-4b6c-9aec-831eb7f1c6ca
  Last attempt @ 2013-02-21 10:16:13 was successful.
DC=ForestDnsZones,DC=Adatum,DC=com
  Default-First-Site-Name\LON-DC1 via RPC
  DSA object GUID: 10876980-527c-4b6c-9aec-831eb7f1c6ca
  Last attempt @ 2013-02-21 10:15:53 was successful.
  
```

- Im Eventlog des geklonten DCs sind Ereignisse protokolliert, die das Ergebnis bestätigen:



- In meiner LAB-Umgebung hat der Prozess vom Start der VM bis zur vollständigen Replikation ca. 5 Minuten gedauert