



Windows Server 2012 R2

Active Directory Domain Services

Active Directory Domain Services 2012 R2 -
Grundinstallation

Active Directory Domain Services 2012 R2 - Grundinstallation

Inhalt

Windows Server Vorbereitung	2
Wissenswertes und Vorbereitungen für neue Domain Controller	2
Active Directory Domänendienste installieren	3

Windows Server Vorbereitung

Um dieses HowTo schreiben zu können, wurde das Ganze in einer Virtuellen Umgebung mit Oracle VM VirtualBox nachgestellt.

- ↳ Microsoft Windows Server 2012 R2 (Deutsch)
- ↳ Microsoft .NET Framework 3.5 SP 1 - Server Feature
- ↳ Windows Updates (ca. 320)
- ↳ Active Directory Domänendienste - Server Rolle

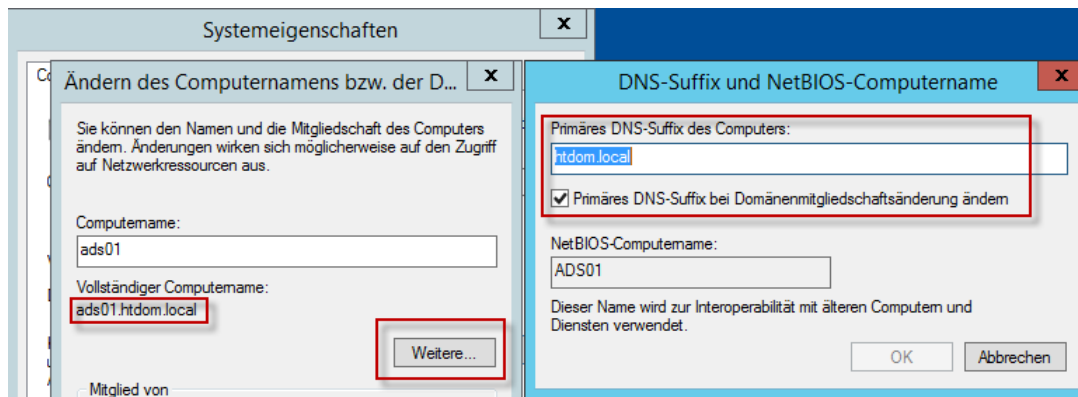
Wissenswertes und Vorbereitungen für neue Domain Controller

Folgende Dinge sollte man beachten, bevor man Domain Controller im Netzwerk bereitstellt.

- ↳ Es sollten vorab alle Windows Updates auf dem Server installiert sein.
- ↳ Der neue Domaincontroller sollte immer über eine Statische IP-Adresse verfügen.
- ↳ Die Server sollte bereits den passenden Hostnamen konfiguriert haben, spätere Änderungen sind nicht sehr förderlich und sorgen nur für Mehraufwand.
- ↳ Das Primäre DNS-Suffix sollte vor der Hochstufung zum Domain Controller gesetzt sein.
- ↳ Der Domain Controller sollte nach der Installation Zugriff zu einer internen oder externen Zeitquelle (NTP Server) haben.

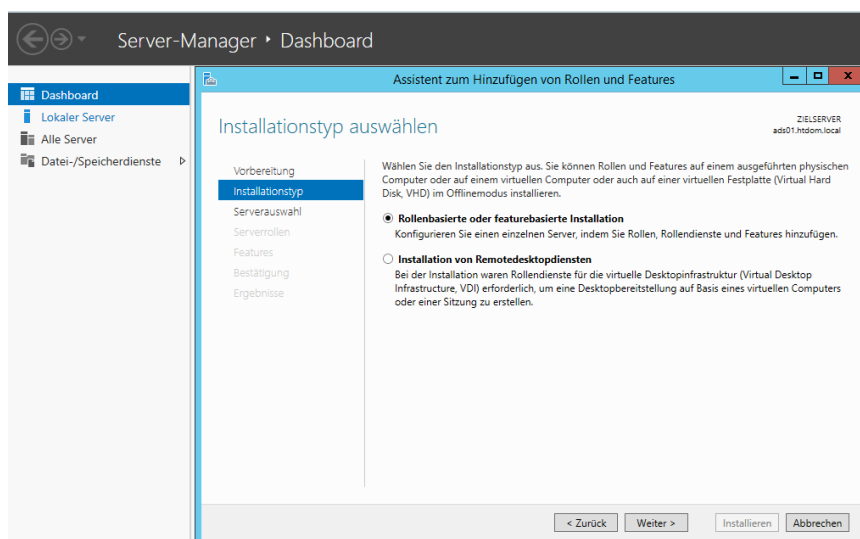
Active Directory Domänendienste installieren

Wie weiter oben bereits angesprochen wird der Server für die Installation von Active Directory vorbereitet in dem man das DNS-Suffix des Computers fest definiert.

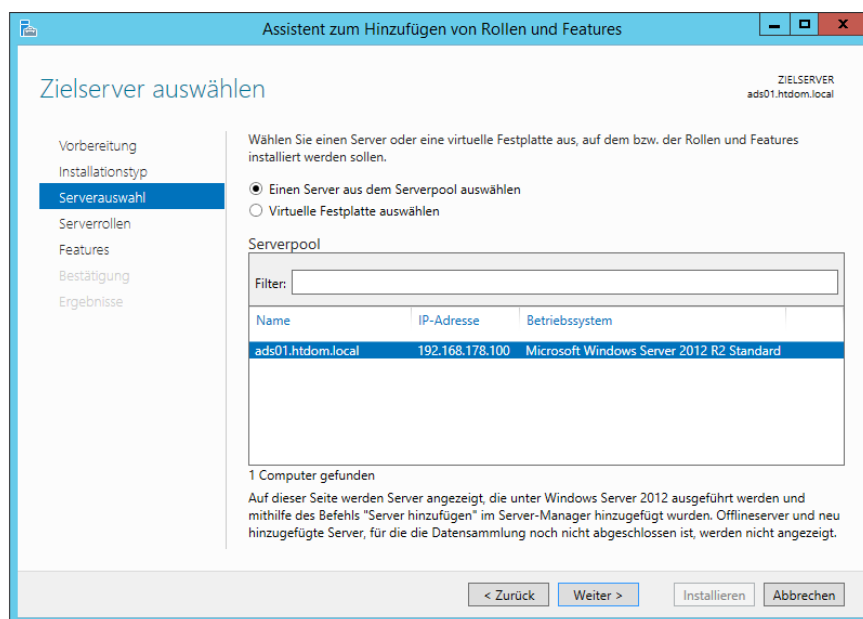


Wenn wir alle Vorbereitungen wie oben beschrieben getroffen haben, können wir die Server Rolle - Active Directory Domänendienste installieren.

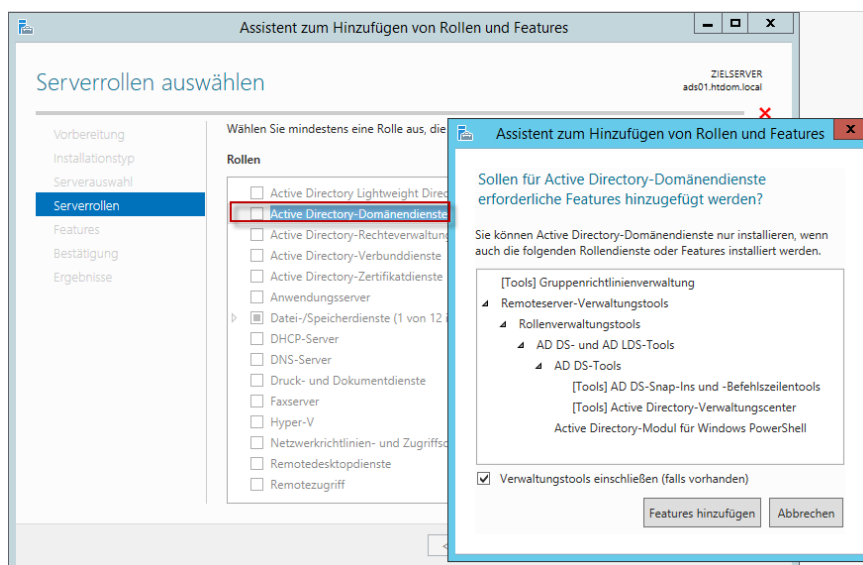
Dazu starten wir den Server Manager --> Verwalten --> Rollen und Features hinzufügen.



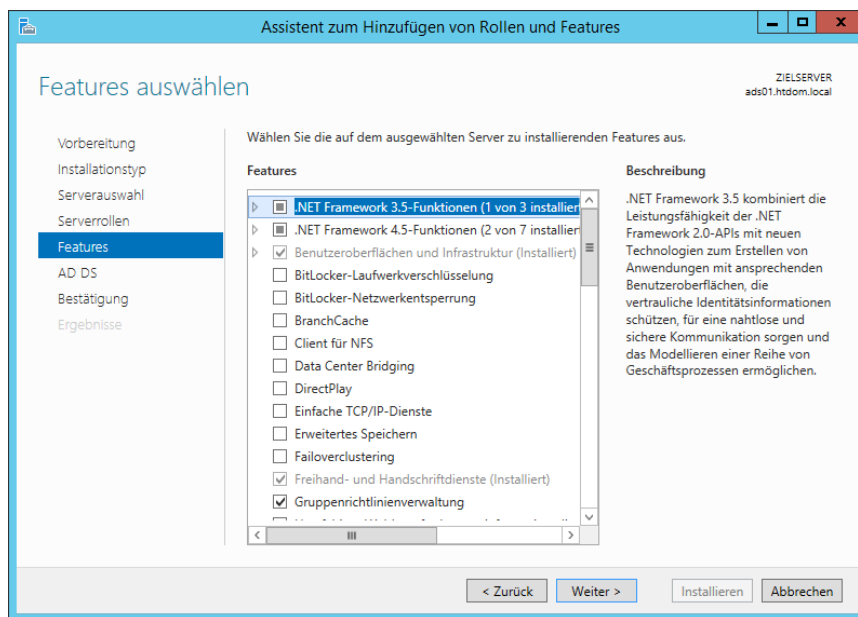
Klicken im Assistenten auf Weiter.



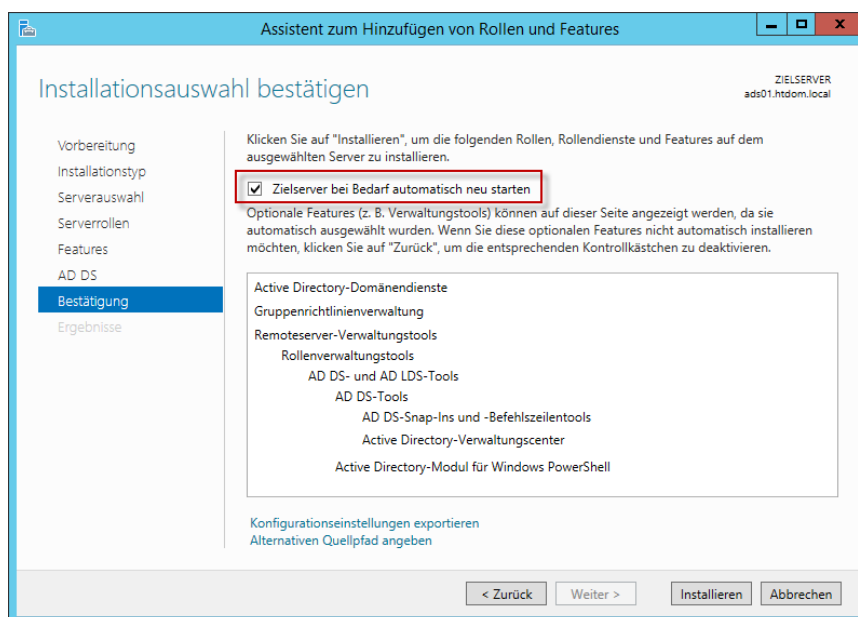
Wählen den Servernamen aus auf dem die Server Rolle installiert werden soll und klicken ebenfalls auf Weiter.



In der Liste wählen wir die **Active Directory Domänendienste** aus und bestätigen die erforderliche Feature Installation mit **Feature hinzufügen**.

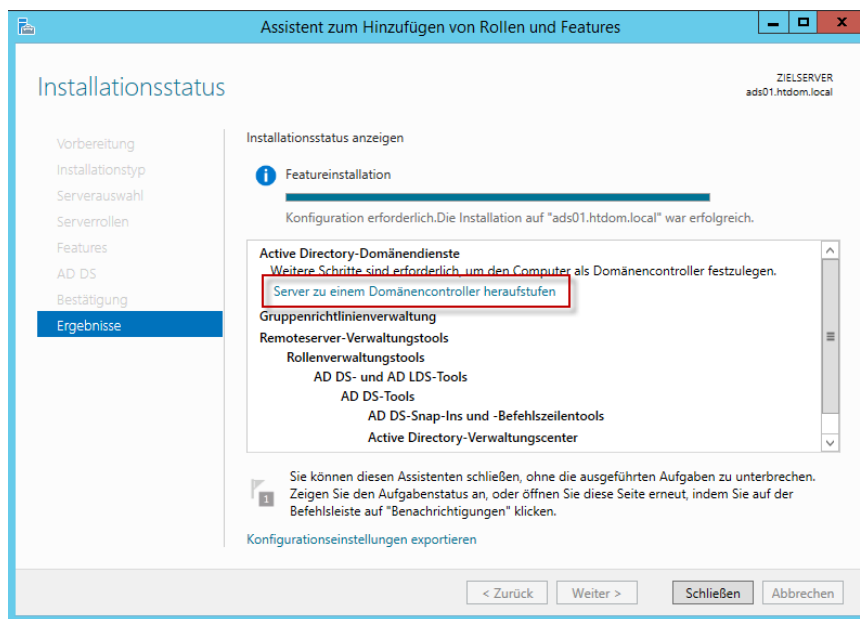


Da wir bereits alle Feature für die Rollen Installation hinzugefügt haben, klicken wir auf Weiter.

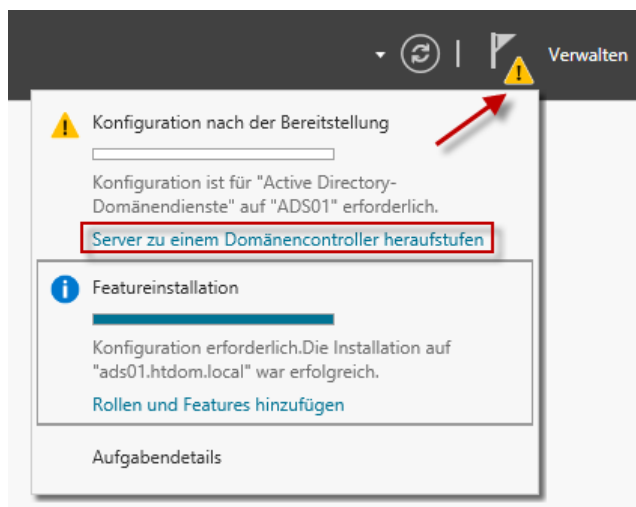


Da dies der erste Domänen Controller in der Domain ist, darf dieser nach der Installation automatisch neu starten. (*Diese Einstellung ist optional*), wenn alle Einstellungen passen, können wir auf Installieren klicken.

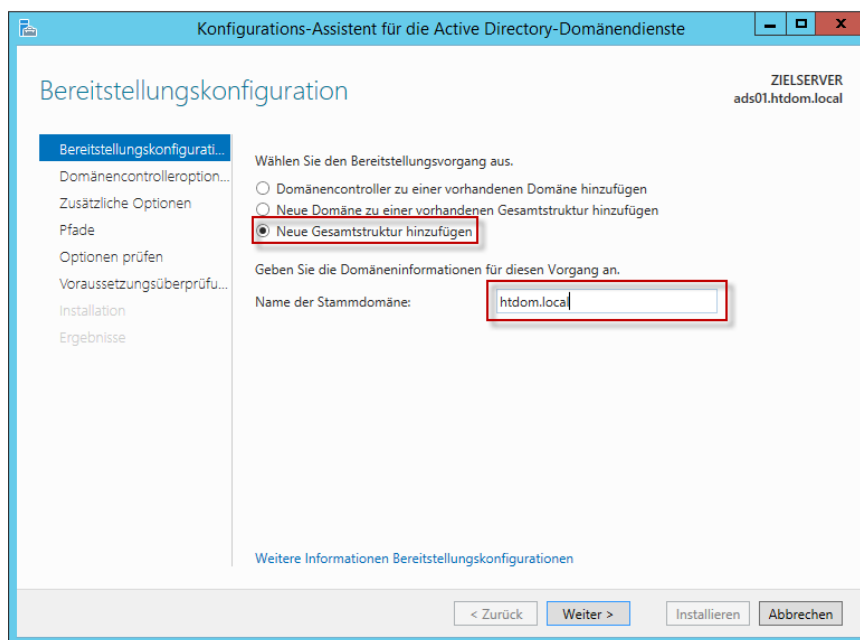
Nun wird der Server für die Active Directory Serverrolle vorbereitet.



Nachdem wir auf Installieren geklickt haben, kann man den Konfigurationsassistenten schließen oder wartet kurze Zeit und klickt dann auf dem Link um den Server heraufzustufen, sollte das Konfigurationsassistenten Fenster bereits geschlossen worden sein.

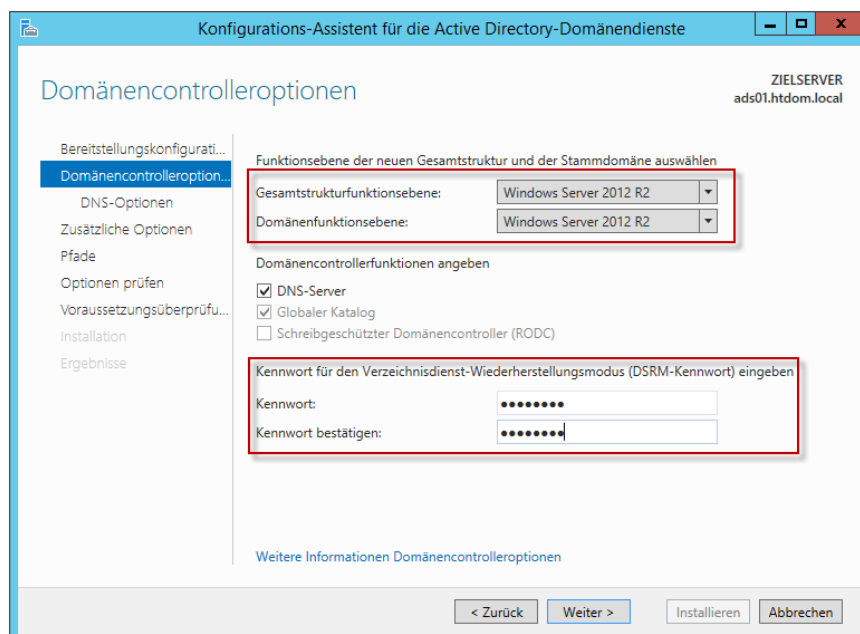


Findet man im Server Manager ein kleines Gelbes Ausrufezeichen, das weitere Aktionen ankündigt. Hierzu klickt man auf den Eintrag "**Server zu einem Domänencontroller heraufstufen**"



Nun öffnet sich ein weiterer Konfigurationsassistent, in diesem Fenster wählt man eine **Neue Gesamtstruktur hinzufügen** aus und vergibt seinen eigenen Domänennamen.

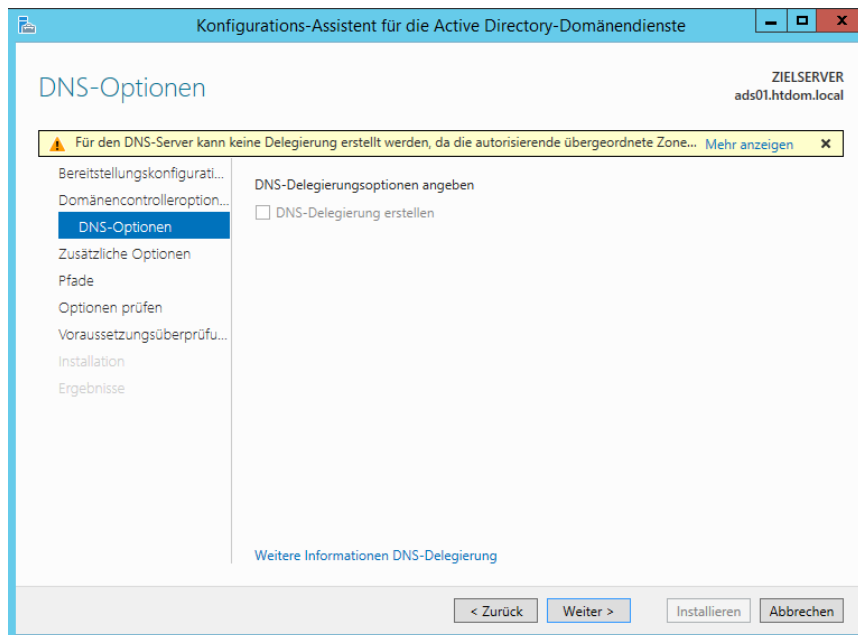
htdom.local (Hat folgende Bedeutung, **ht** steht für Helmut Thurnhofer, **dom** ist eine Abkürzung für Domain und **local** steht für Test Domäne, hier kann man anstelle local auch gerne de/at/ch/com/net/inc/int/intern nutzen, seit kreativ bei der Namensgebung)



Da dies der erste Domain Controller im Netzwerk ist, kann die Gesamtfunktions- und Domänenfunktionsebene auf Windows Server 2012 R2 stehen bleiben, diese Einstellung würde nur relevant werden, wenn dieser Server einen älteren Server 2008/2008 R2/2012 ablösen sollte.

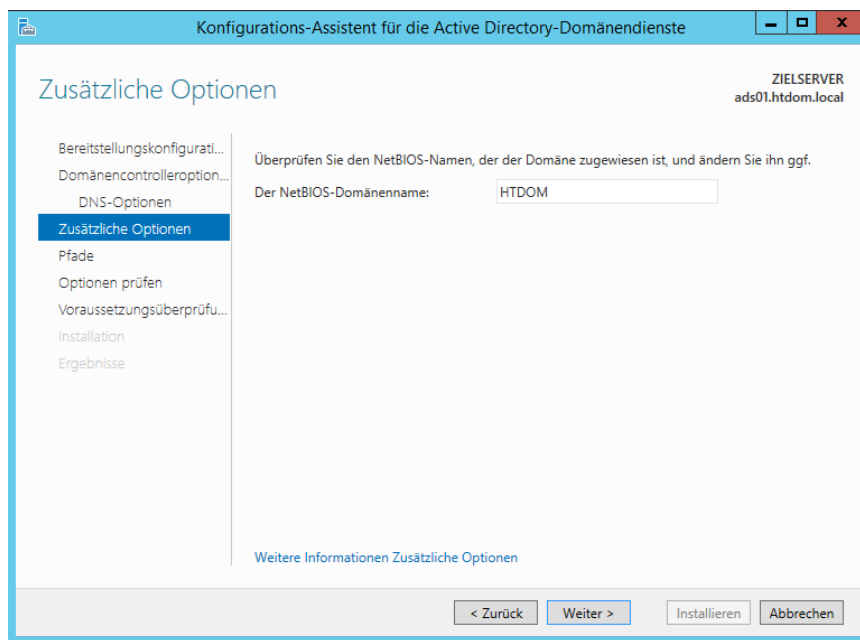
Ist aber in diesen Howto nicht von Bedeutung, was aber sehr wichtig ist, ist das DSRM Passwort das man hier vergibt. Dieses wird benötigt wenn man mal irgendwann in zwei/drei Jahren einen Ausfall zu beklagen hat und den Domaincontroller wiederherstellen muss.

Daher sollte dieses Passwort sicher aufbewahrt (Firmtresor, Disaster Recovery Planung) werden. Dieses Passwort hat nichts mit den Domänen Administrator Passwort zu tun. Sollte man das Passwort doch einmal vergessen haben, kann man dieses jeder Zeit per **ntdsutil** zurücksetzen werden. DSRM steht in diesen Zusammenhang für **Directory Services Restore Mode**.



Im nächsten Schritt kommen die DNS-Optionen, hier klicken wir auf Weiter und ignorieren die DNS-Delegationsoptionen, da dies unser erster Domain Controller ist können wir diesen Namensraum nicht selbst delegieren.

Diese Einstellung würde nur relevant werden, sobald wir Subdomains einrichten, diese neuen Namensräume würden dann in die den Hauptnamensraum delegiert.



Der NetBIOS Name wird automatisch vom Assistent aufgelöst und eingetragen, wenn man diesen verändern möchte, kann man dies gerne machen. Diese Einstellung beeinflusst das spätere Prä-Windows 2000 Anmeldeverhalten an der Domäne.

Beispiel hier wäre folgende Konstellation:

FQDN Anmeldung = *net.ht-firmenname.de* = *username@net.ht-firmenname.de*

NetBIOS Anmeldung = *HT* = *ht\username*

Benutzeranmeldename:

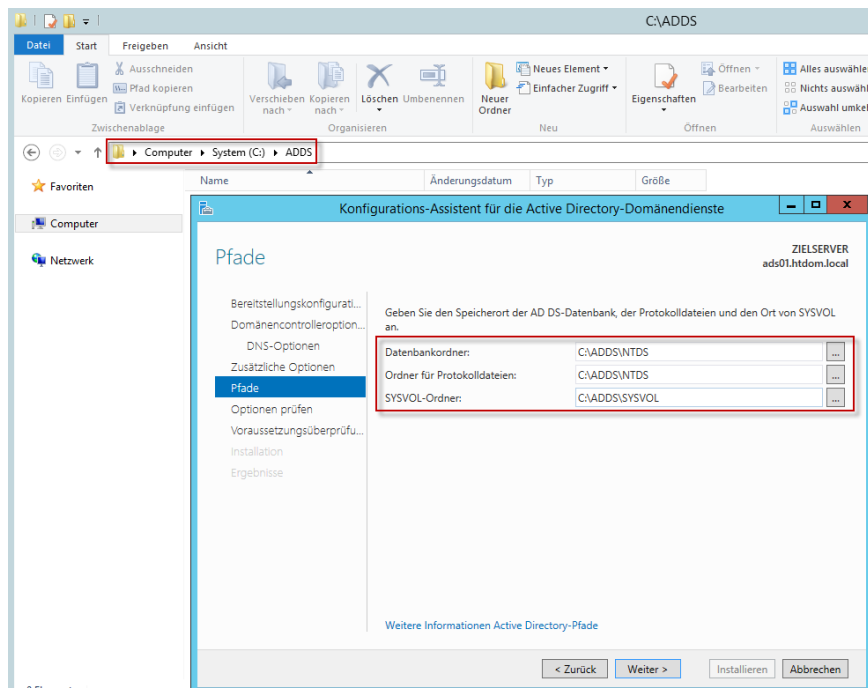
Benutzeranmeldename (Prä-Windows 2000):

Geben Sie den Speicherort der AD DS-Datenbank, der Protokolldateien und den Ort von SYSVOL an.

Datenbankknoten: C:\Windows\NTDS

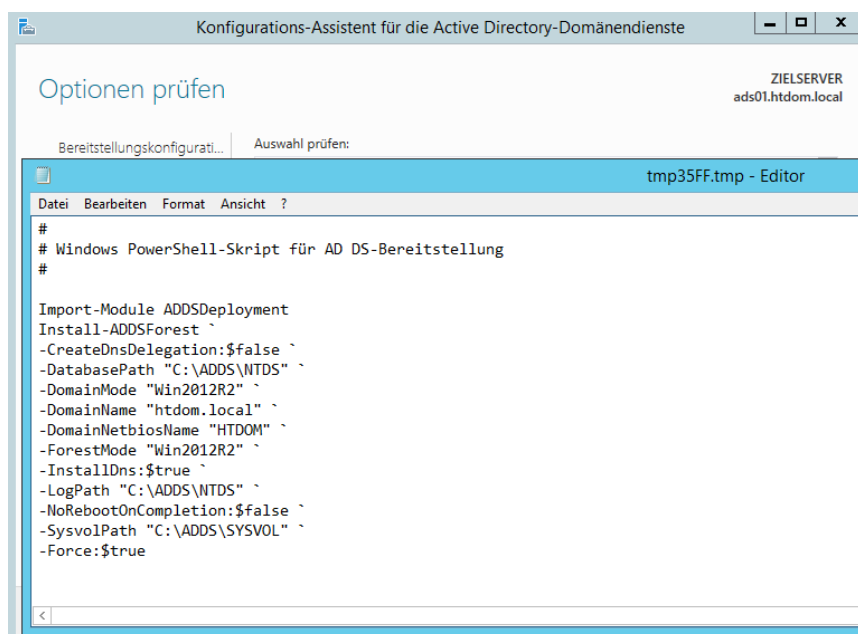
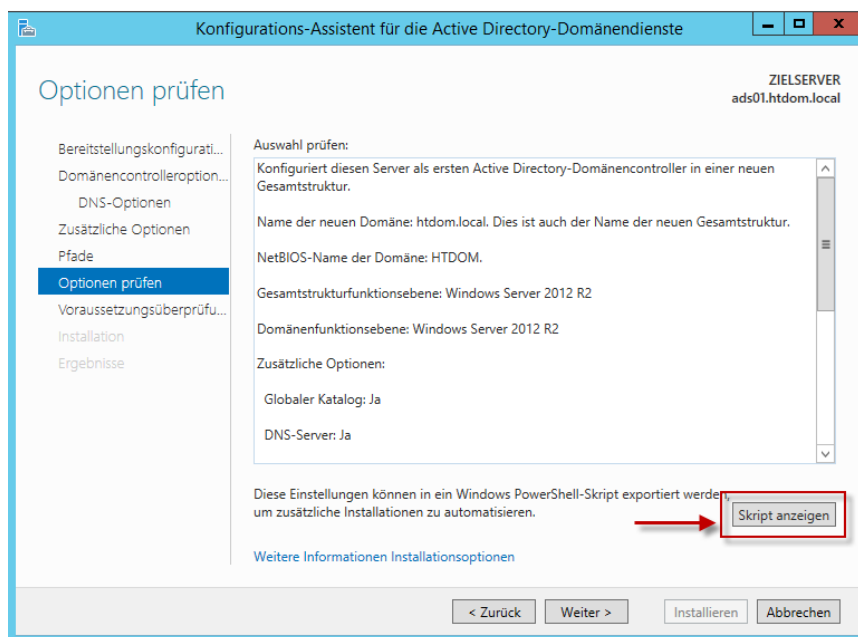
Ordner für Protokolldateien: C:\Windows\NTDS

SYSVOL-Ordner: C:\Windows\SYSVOL



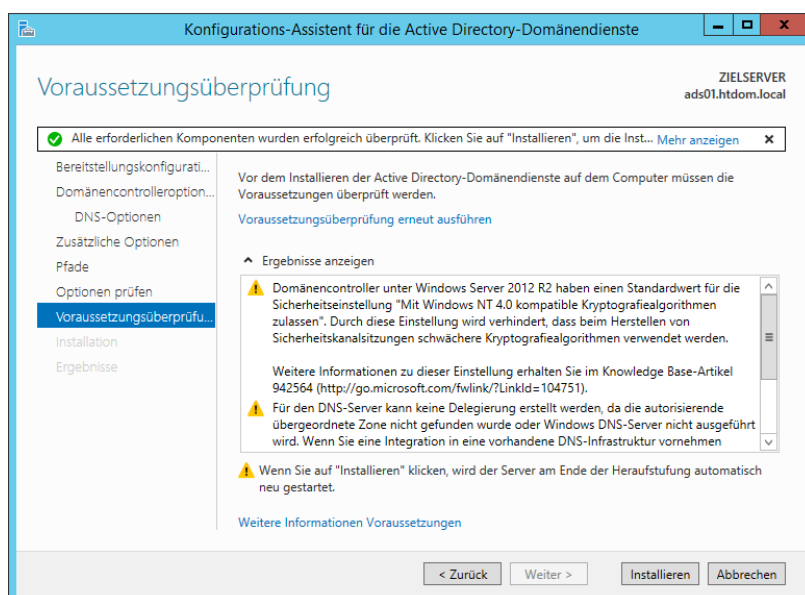
Microsoft Best Practice sagt, das man die Pfadangaben im Standard stehen lassen sollte. Außer es existiert im Server eine schnellere Partition/Festplatte (wie z.B. eine SSD oder RAID Verbund) dann kann man hier die Pfade dahingehend anpassen, der Zugriff auf die NTDS.dit Datenbank wird dadurch schneller.

Habe mir aber schon vor Jahren angewöhnt die Pfade hier anzupassen. Glaube dass es mittlerweile Geschmacksache ist, sollte man in einem Kundensysteme die Möglichkeit haben eine neue AD Struktur aufzubauen, dann würde ich hier den Standardpfad empfehlen, ist es aber eine Testumgebung, dann kann man hier ein bisschen experimentieren.

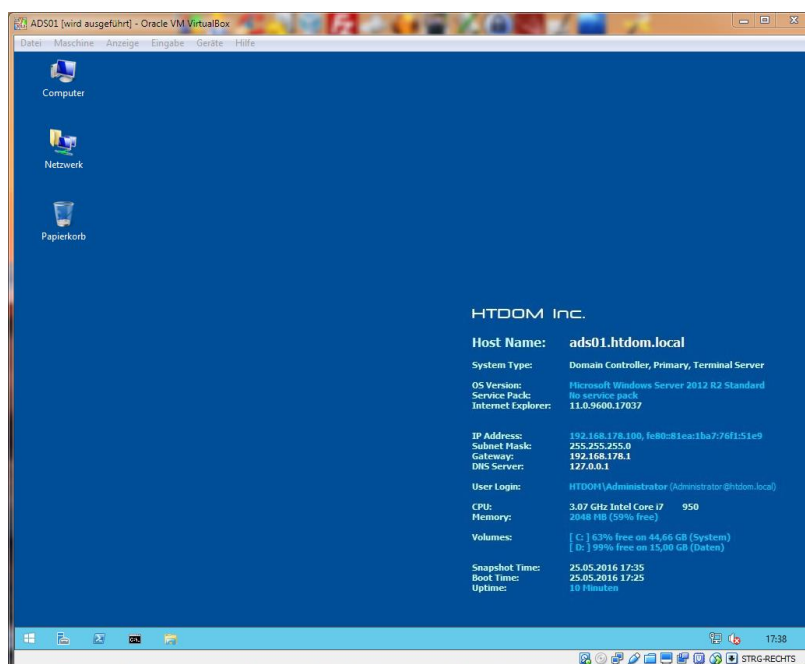


Die Gesamtübersicht sehe ich mir nochmal genauer an und lass mir bevor ich auf weiter klicke, das PowerShell Skript anzeigen, dieses könnte man sich lokal abspeichern um spätere Domain Controller über die PowerShell installieren zu können.

Für den Übungszweck sehr interessant, persönlich klicke ich mich aber gerne durch den Assistenten um die Kontrolle zu behalten.



Es werden vom Assistent noch alle Voraussetzungen überprüft, hier werden auch ein paar Warnungen ausgegeben, diese sollte man sich nur zu Herzen nehmen, wenn es in der Umgebung noch Windows NT 4.0 Domänen gibt, da wir hier aber eine neue Gesamtstruktur aufbauen, kann man die Meldung getrost ignorieren, die zweite Meldung kennen wir ebenfalls und wissen das wir für die Hauptdomain keine DNS-Delegation einrichten können.



Nachdem die Server Rolle installiert wurde, startet der Server automatisch neu und nach dem Neustart kann man sich als Domänen Administrator an dem Server anmelden.

Viele Grüße
Helmut Thurnhofer