

Administrator Praxis
Microsoft Deployment Toolkit (MDT) 2013 Update 2

Windows 10 & Windows Server 2016 ready

Kapitel 21:

PXE-Boot mit UEFI

21

PXE-Boot mit UEFI

Mittlerweile löst UEFI (Unified Extensible Firmware Interface) schrittweise das immer noch weit verbreitete BIOS (Basic Input/ Output System) als grundlegende Firmware für PCs und Server ab. Mit dieser hochflexiblen, modernen Firmware kommen neue Funktionen und Möglichkeiten, wie zum Beispiel Secure Boot.

Secure Boot erlaubt nur noch signierte Bootloader, um beispielsweise Schadsoftware daran zu hindern, den Startvorgang zu manipulieren.

Unter Hyper-V haben Sie dafür die Generation 2 VMs. Der Bootvorgang über das Netzwerk und PXE funktioniert hier auf andere Art und Weise. Damit muss auch die beschriebene Vorgehensweise aus Kapitel 14 angepasst werden.

Falls Sie ein kleines Netzwerk haben, das mit einem IP-Bereich auskommt und Sie auch keine VLANs benutzen, verwenden Sie ruhig die beschriebene Vorgehensweise. Diese funktioniert in der Regel sehr gut. In den anderen Fällen verwenden Sie die IP-Helfer-Funktion Ihrer Switches. Details können Sie unter

<https://techcommunity.microsoft.com/t5/Configuration-Manager-Blog/You-want-to-PXE-Boot-Don-t-use-DHCP-Options/ba-p/275562>
sowie im jeweiligen Handbuch Ihrer Switches nachlesen.

21.1 DHCP Herstellerklassen erstellen

HINWEIS:

Beachten Sie, dass es zwingend bei diesem, im Folgenden beschriebenen, Vorgehen eine Trennung zwischen dem DHCP- und dem WDS-Server geben muss. Falls beide Rollen auf einem Server sind, funktioniert es nicht!

Im Blog-Eintrag¹ von Mike Galvin² ist die Vorgehensweise detailliert beschrieben. Zuerst ist es notwendig, drei neue Herstellerklassen im DHCP-Server zu definieren, falls Sie sowohl BIOS-Rechner, als auch UEFI-Rechner mit 32- und 64 Bit installieren wollen, respektive müssen. Öffnen Sie dazu die DHCP-Verwaltungskonzole als Administrator. Im Kontextmenü des DHCP-Servers finden Sie den Menüpunkt „Herstellerklassen definieren...“.

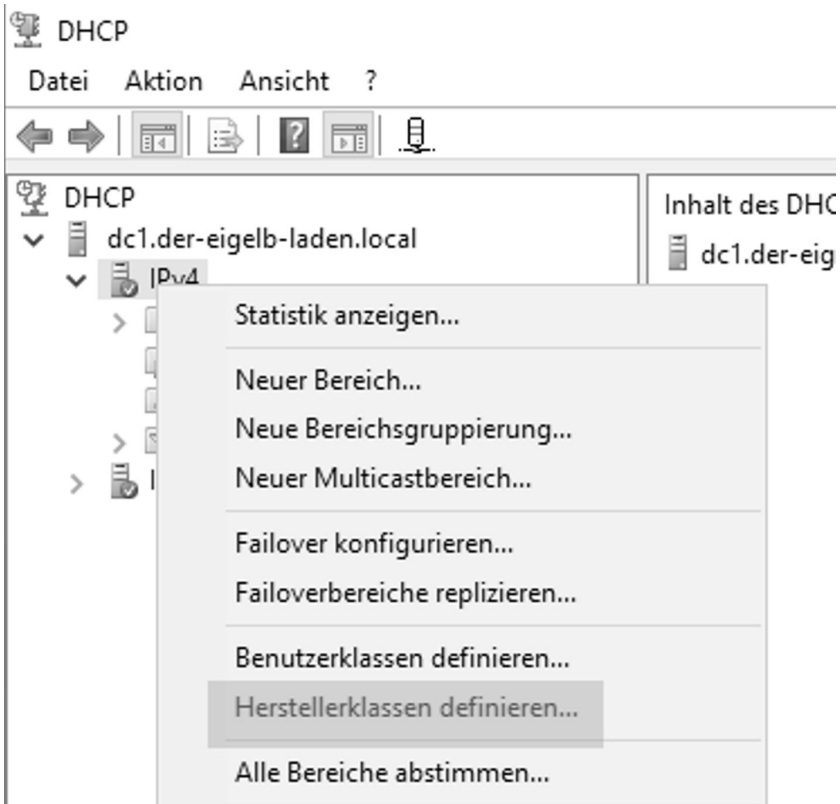


Abbildung 21.1: Eine neue Herstellerklasse

Klicken Sie auf „Hinzufügen...“ und vergeben Sie einen aussagekräftigen Anzeigenamen sowie eine Beschreibung (hier: PXEClient (UEFI x64)).

¹ <https://gal.vin/2017/05/05/pxe-booting-for-uefi-bios/>

² <https://social.technet.microsoft.com/profile/mike%20galvin>

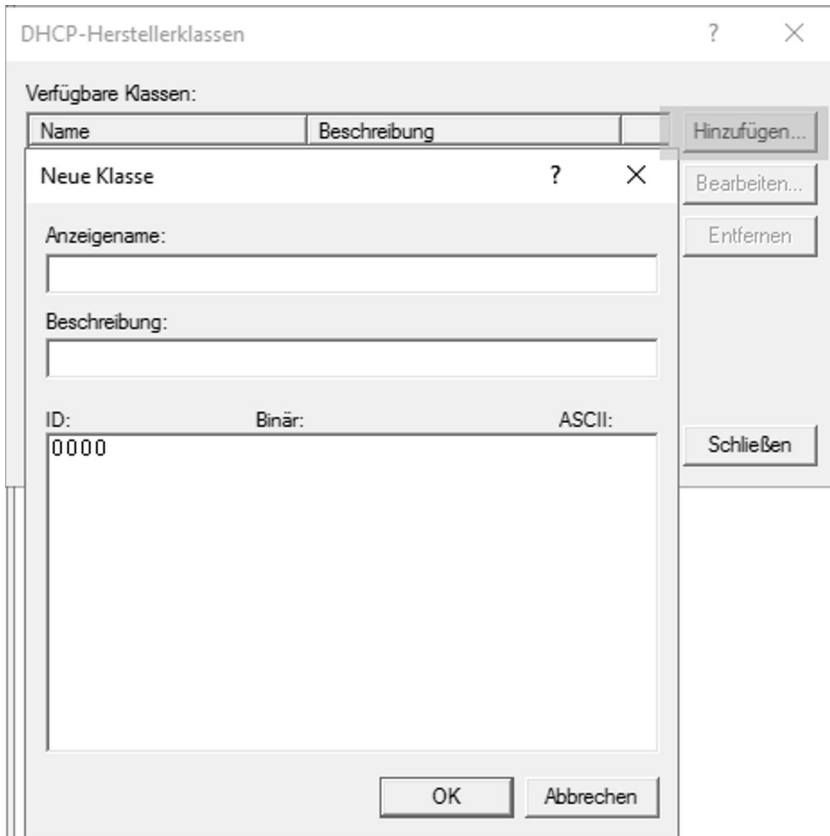


Abbildung 21.2: Hinzufügen einer weiteren Herstellerklasse

Fügen Sie folgende Inhalte der ASCII-Sektion hinzu:
PXEClient:Arch:00007

Beachten Sie an dieser Stelle Groß- und Kleinschreibung. Hier ist es nicht möglich, die Inhalte per „Kopieren-und-Einfügen“ einzutragen. Daher prüfen Sie bitte Ihre Einträge auf Korrektheit.

Neue Klasse?×

Anzeigename:

Beschreibung:

ID:	Binär:	ASCII:
0000	50 58 45 43 6C 69 65 6E	PXEClient
0008	74 3A 41 72 63 68 3A 30	t:Arch:0
0010	30 30 30 37	0007

OK

Abbrechen

Abbildung 21.3: Eingetragene Werte in der Tabelle

Vollziehen Sie ggfs. die gleichen Schritte für UEFI x86 mit den ASCII-Werten **PXEClient:Arch:00006** und BIOS mit den ASCII-Werten **PXEClient:Arch:00000**

Am Ende sollten Sie nun drei neue Einträge bei den Herstellerklassen haben.

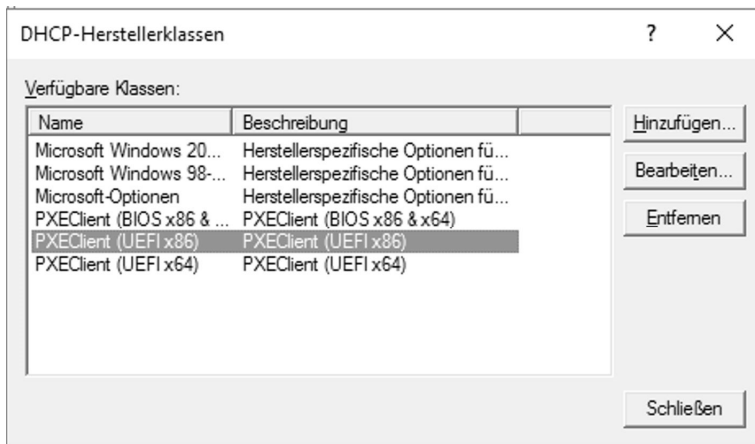


Abbildung 21.4: Drei neue Herstellerklassen

21.2 DHCP-Richtlinien erstellen

Im weiteren Schritt benötigen wir DHCP-Richtlinien. Diese können entweder auf Server- oder Bereichsebene erstellt werden.

Rufen Sie dazu das Kontextmenü der Richtlinien im definierten IP-Bereich auf und wählen Sie „Neue Richtlinie...“.

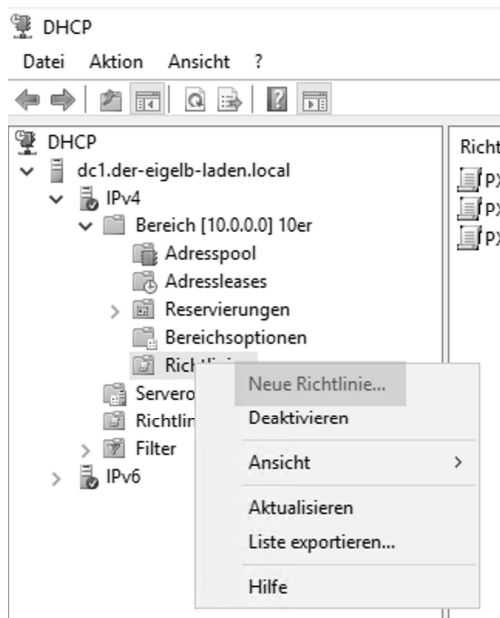


Abbildung 21.5: Erstellen einer neuen Richtlinie

Vergeben Sie auch hier einen aussagekräftigen Namen (hier: PXEClient (UEFI x64)).

Konfigurations-Assistent für DHCP-Richtlinien

Richtlinienbasierte Zuweisung von IP-Adressen und Optionen

Dieses Feature ermöglicht das Verteilen konfigurierbarer Einstellungen (IP-Adresse, DHCP-Optionen) an Clients auf der Grundlage bestimmter Bedingungen wie Herstellerklasse, Benutzerklasse, MAC-Adresse usw.

Dieser Assistent unterstützt Sie beim Einrichten einer neuen Richtlinie. Geben Sie einen Namen (beispielsweise "Konfigurationsrichtlinie für VoIP-Telefon") sowie eine Beschreibung (beispielsweise "NTP-Option für VoIP-Telefone") für die Richtlinie an.

Richtlinienname:

Beschreibung:

< Zurück Weiter > Abbrechen

Abbildung 21.6: Konfiguration der Richtlinie Schritt 1

Klicken Sie auf „Hinzufügen...“

Bedingungen für die Richtlinie konfigurieren



Eine Richtlinie besteht aus mindestens einer Bedingung sowie aus Konfigurationseinstellungen (Optionen, IP-Adresse), die an den Client verteilt werden. Diese Einstellungen werden vom DHCP-Server an Clients übertragen, die den Bedingungen entsprechen.

- ! Für eine Richtlinie mit Bedingungen, die auf dem vollqualifizierten Domännennamen basieren, können Konfigurationseinstellungen für DNS angegeben werden, jedoch nicht für Optionen oder IP-Adressbereiche.

Bedingungen	Operator	Wert

☐ UND

☒ ODER

Hinzufügen...

Bearbeiten...

Entfernen

< Zurück

Weiter >

Abbrechen

Abbildung 21.7: Konfiguration der Richtlinie Schritt 2

Wählen Sie aus dem Dropdown-Menü Ihre vorhin erstellte Herstellerklasse aus, setzen Sie den Haken bei „Platzhalter anfügen (*)“ und fügen Sie diese Bedingung hinzu.

Bedingung hinzufügen/bearbeiten

Geben Sie eine Bedingung für die zu konfigurierende Richtlinie an. Wählen Sie ein Kriterium, einen Operator sowie Werte für die Bedingung aus.

Kriterien: Herstellerklasse

Operator: Ist gleich

Wert(e)

Wert: PXEClient (UEFI x64)

☐ Platzhalter voranstellen(*)

☒ Platzhalter anfügen(*)

Hinzufügen

Entfernen

OK

Abbrechen

Abbildung 21.8: Konfiguration der Richtlinie Schritt 3

Bedingungen für die Richtlinie konfigurieren



Eine Richtlinie besteht aus mindestens einer Bedingung sowie aus Konfigurationseinstellungen (Optionen, IP-Adresse), die an den Client verteilt werden. Diese Einstellungen werden vom DHCP-Server an Clients übertragen, die den Bedingungen entsprechen.

- ! Für eine Richtlinie mit Bedingungen, die auf dem vollqualifizierten Domännennamen basieren, können Konfigurationseinstellungen für DNS angegeben werden, jedoch nicht für Optionen oder IP-Adressbereiche.

Bedingungen	Operator	Wert
Herstellerklasse	Ist gleich	PXEClient (UEFI x64)*

☐ UND

☒ ODER

Hinzufügen...

Bearbeiten...

Entfernen

< Zurück

Weiter >


Abbrechen

Abbildung 21.9: Konfiguration der Richtlinie Schritt 4

Klicken Sie auf „Weiter >“.

Ändern Sie den Radio-Button von „Ja“ zu „Nein“ und navigieren Sie zum nächsten Menü.

Konfigurations-Assistent für DHCP-Richtlinien

Einstellungen für die Richtlinie konfigurieren


Entsprechen die in der Richtlinie angegebenen Bedingungen einer Clientanforderung, werden die Einstellungen angewendet.

Ein Bereich kann in mehrere IP-Adressbereiche unterteilt sein. Clients, von denen die in einer Richtlinie definierten Bedingungen erfüllt werden, erhalten eine IP-Adresse aus dem angegebenen Bereich.

Konfigurieren Sie die Start- und End-IP-Adresse für den Bereich. Start- und End-IP-Adresse für den Bereich müssen innerhalb der Start- und End-IP-Adresse für den Geltungsbereich liegen.

Der aktuelle Bereich besitzt den folgenden IP-Adressbereich: 10.10.10.100 - 10.20.0.0

Ist für die Richtlinie kein IP-Adressbereich konfiguriert, erhalten Richtlinienclients eine IP-Adresse aus dem Bereich des Geltungsbereichs.

Möchten Sie einen IP-Adressbereich für die folgende Richtlinie konfigurieren? ☐ Ja ☒ Nein

Start-IP-Adresse:

End-IP-Adresse:

Prozentsatz des IP-Adressbereichs: %

Es wurde kein gültiger Bereich angegeben.

Abbildung 21.10: Konfiguration der Richtlinie Schritt 5

Suchen Sie nun die Option 60, setzen Sie den Haken und tragen Sie als Zeichenfolgenwert „PXEClient“ ein.

Konfigurations-Assistent für DHCP-Richtlinien

Einstellungen für die Richtlinie konfigurieren

Entsprechen die in der Richtlinie angegebenen Bedingungen einer Clientanforderung, werden die Einstellungen angewendet.



Herstellerklasse:

Zur Verfügung stehende Optionen	Beschreibung
<input type="checkbox"/> 049 X Window-Systemanzeige	Array von X Windows-Anzeiges
<input checked="" type="checkbox"/> 060 PXEClient	PXE
<input type="checkbox"/> 064 NIS+-Domänenname	Der Name der NIS+-Domäne de

< >

Dateneingabe

Zeichenfolgenwert:

< Zurück Weiter > Abbrechen

Abbildung 21.11: Konfiguration der Richtlinie Schritt 6

Scrollen Sie anschließend weiter zu Option 66. Setzen Sie auch hier den Haken und tragen Sie an dieser Stelle die IP-Adresse des WDS-Servers ein (hier: 10.10.10.10.11). Alternativ können Sie auch den FQDN des Servers angeben.

Einstellungen für die Richtlinie konfigurieren

Entsprechen die in der Richtlinie angegebenen Bedingungen einer Clientanforderung, werden die Einstellungen angewendet.



Herstellerklasse: DHCP Standard Options

Zur Verfügung stehende Optionen	Beschreibung
<input type="checkbox"/> 064 NIS+-Domänenname	Der Name der NIS+-Domäne de
<input type="checkbox"/> 065 NIS+-Server	Eine Liste von IP-Adressen, die
<input checked="" type="checkbox"/> 066 Hostname des Startservers	Hostname des TFTP-Startserve

< >

Dateneingabe

Zeichenfolgenwert:

10.10.10.11

< Zurück Weiter > Abbrechen

Abbildung 21.12: Konfiguration der Richtlinie Schritt 7

Bei Option 67 setzen Sie ebenfalls den Haken und tragen als Zeichenfolgenwert „boot\x64\wdsimgfw.efi“ ein.

Konfigurations-Assistent für DHCP-Richtlinien

Einstellungen für die Richtlinie konfigurieren
 Entsprechen die in der Richtlinie angegebenen Bedingungen einer Clientanforderung, werden die Einstellungen angewendet.

Herstellerklasse: DHCP Standard Options

Zur Verfügung stehende Optionen	Beschreibung
<input checked="" type="checkbox"/> 066 Hostname des Startservers	Hostname des TFTP-Startserve
<input checked="" type="checkbox"/> 067 Name der Startdatei	Name der Startdatei
<input type="checkbox"/> 068 Mobile IP-Home-Agents	Mobile IP-Home-Agents in Priori

< >

Dateneingabe

Zeichenfolgenwert:

boot\x64\wdsmgfw.efi

< Zurück
Weiter >
Abbrechen

Abbildung 21.13: Konfiguration der Richtlinie Schritt 8

Schließen Sie den Assistenten ab.

Zusammenfassung

Eine neue Richtlinie wird mit den folgenden Einstellungen erstellt. Zeigen Sie zum Konfigurieren von DNS-Einstellungen die Eigenschaften der Richtlinie an, und klicken Sie auf die Registerkarte "DNS".

Name: jklqehö

Beschreibung:

Bedingungen: ODER von

Bedingungen	Operator	Wert
Herstellerklasse	Ist gleich	PXECient (UEFI x64)*

Einstellungen

Optionsname	Herstellerklasse	Wert
PXECient		PXECient
Hostname des Startservers		10.10.10.11
Name der Startdatei		boot\x64\wdsmgfw.efi

< Zurück

Fertig stellen

Abbrechen

Abbildung 21.14: Konfiguration der Richtlinie Abschluss

Sollten Sie noch UEFI x86 oder BIOS, sowohl 32 als auch 64 Bit unterstützen wollen/ müssen, dann wiederholen Sie diese neun Schritte.

Die Namen der Startdateien sind an dieser Stelle dann „boot\x86\wdsmgfw.efi“ für UEFI x86 und „boot\x64\wdsnbp.com“ für BIOS.

Damit sind die Richtlinien konfiguriert.

In der DHCP-Verwaltungskonsole unter „Bereichsoptionen“ sehen Sie in der Übersicht alle Ihren definierten Richtlinien.

DHCP		Optionsname	Hersteller	Wert	Richtli
dc1.der-eigelt-laden.local		060 PXEClient	Standard	PXEClient	PXEClient
IPv4		066 Hostname des Startservers	Standard	10.10.10.11	PXEClient
Bereich [10.0.0.0] 10er		067 Name der Startdatei	Standard	boot\x64\wdsmsgfw.efi	PXEClient
Adresspool		060 PXEClient	Standard	PXEClient	PXEClient
Adressleases		066 Hostname des Startservers	Standard	10.10.10.11	PXEClient
Reservierungen		067 Name der Startdatei	Standard	boot\x86\wdsmsgfw.efi	PXEClient
Bereichsoptionen		060 PXEClient	Standard	PXEClient	PXEClient
Richtlinien		066 Hostname des Startservers	Standard	10.10.10.11	PXEClient
Serveroptionen		067 Name der Startdatei	Standard	boot\x86\wdsnbp.com	PXEClient
Richtlinien		003 Router	Standard	10.10.10.10	Keine
Filter		006 DNS-Server	Standard	10.10.10.10	Keine
IPv6					

Abbildung 21.15: Konfigurierte Bereichsoptionen

Wenn Sie jetzt eine VM oder einen Rechner mit aktiviertem Secure Boot starten und als Boot-Option „Netzwerkboot“ auswählen, wird die VM oder der Rechner die jeweils korrekte Startdatei erhalten und sich dann über den WDS mit dem MDT-Server verbinden.



Abbildung 21.16: Netzwerkboot mit UEFI

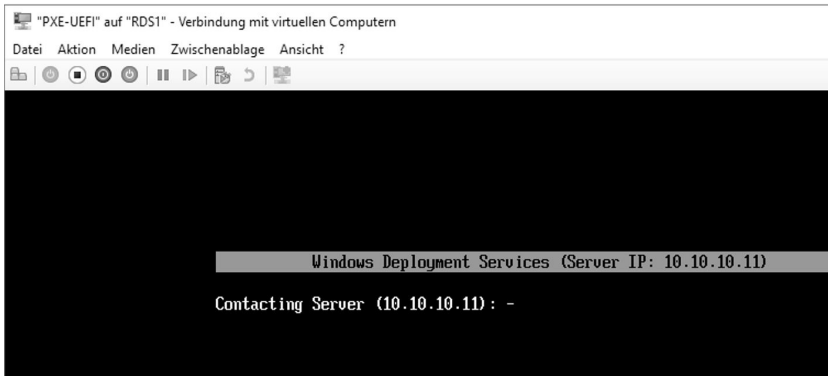


Abbildung 21.17: UEFI Boot

Bei älteren VMs oder Rechnern werden dementsprechend die anderen Startdateien verwendet.

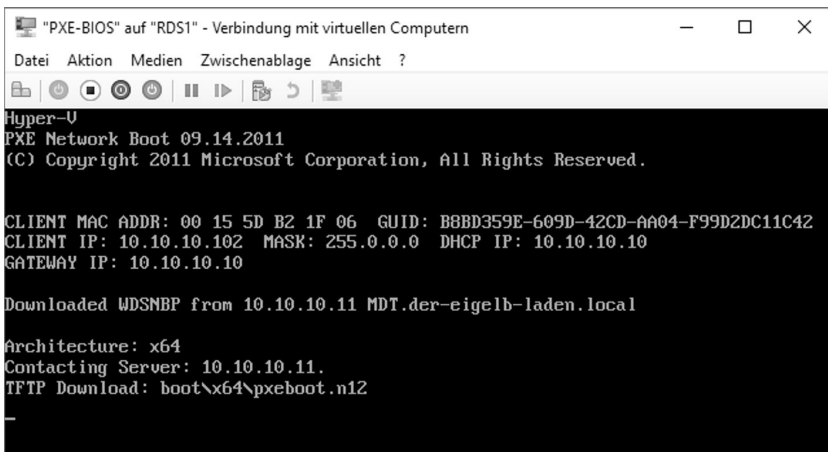


Abbildung 21.18: Ältere VMs/ PCs booten über das Netzwerk