invisAD-setup - action #81076

DHCP-Server Konfiguration im AD so vorbereiten, dass der Server Routen pushen kann.

2020-12-15 19:44 - flacco

Status:	In Progress	**Start date:**	2020-12-15
Priority:	Normal	**Due date:**	2021-12-31
Assignee:	flacco	**% Done:**	30%
Category:	Feature	**Estimated time:**	0.00 hour
Target version:	Future		

Description

Dafür müssen die LDIF-Dateien für das Setup des Servers um zwei DHCP-Optionen erweitert werden:

rfc3442-classless-static-routes code 121 = array of integer 8
ms-classless-static-routes code 249 = array of integer 8

Ergänzend sollte ein Shellscript für die invis-Toolbox geschrieben werden, welches die eigentlichen Routen dann in der Subnetz-Deklaration die eigentlichen Routen ergänzt.

History

#1 - 2020-12-15 19:45 - flacco

Ich habe das ganze einmal manuell durchgeführt und für mich dokumentiert:

Das pushen von Routen via DHCP-Server geschieht in zwei Schritten. Im ersten Schritt müssen in der globalen Konfiguration zwei neue DHCP-Options deklariert werden.

Im ASCII-Setup sind die beiden folgenden Zeilen einzufügen:

option rfc3442-classless-static-routes code 121 = array of integer 8
option ms-classless-static-routes code 249 = array of integer 8

Die doppelte Deklaration ist erforderlich, da sich Windows-Clients anders verhalten als der Rest der Welt.

Anschließend werden die Routen selbst als DHCP-Option bekannt gemacht. Dies kann entweder global, oder innerhalb einer Subnetzdeklaration vorgenommen werden. Merkwürdig ist dabei die Syntax:

option rfc3442-classless-static-routes 16, 188, 144, 192, 168, 230, 73
option ms-classless-static-routes 16, 188, 144, 192, 168, 230, 73

Dabei ist die erste Stelle die Netzmaske des Ziels in CIDR-Schreibweise, danach folgt die Basisadresse des Ziels, ohne Nullen und abschließend die IP-Adresse des Gateways. Dabei werden die IP-Adressen in ihre Bestandteile zerlegt und mit Komma separiert.

Das lässt sich auch im AD-LDAP vornehmen. Dort werden jeweils neue Attribute des Typs „iscDhcpOption“ generiert und die oben dargestellten Informationen ohne das Schlüsselwort „option“ als Wert übergeben.

Knoten für die globalen Options ist:

CN=DHCP Config,CN=DHCP-Server,CN=invis-Server,DC=invis-net,DC=loc

und für die Subnet-Optionen:

CN=xxx.xxx.xxx.0,CN=DHCP Config,CN=DHCP-Server,CN=invis-Server,DC=invis-net,DC=loc

Bei syntaktischen Fehlern auch im AD startet der DHCP-Dienst nicht und gibt leider auch keine brauchbaren Fehlermeldungen aus.

#2 - 2020-12-15 20:07 - flacco

Das Shellscript sollte von vorne herein so aufgebaut werden, dass es sich auch via invis-Portal ausführen lässt.

#3 - 2021-06-17 09:18 - flacco

Ein Script zum Hinzufügen statischer Routen zu den DHCP-Infos im AD ist weit weniger einfach als gedacht. Es gibt zwei zu lösende Fleisaufgaben:

1. Aus der Netzwerkbasisadresse müssen die 0-Bytes eliminiert werden.
2. Werden mehrere statische Routen benötigt müssen weitere Routen an die bereits bestehenden DHCP-Options der ersten Route angehängt und nicht als zusätzliche Optionen eingefügt werden:

rfc3442-classless-static-routes 16, 188, 144, 192, 168, 230, 73, 15, 100, 102, 17, 10, 192, 168, 230, 73
ms-classless-static-routes 16, 188, 144, 192, 168, 230, 73, 15, 100, 102, 17, 10, 192, 168, 230, 73

#4 - 2021-06-17 09:18 - flacco

- % Done changed from 0 to 20

#5 - 2021-06-17 09:23 - flacco

Weiterer Hinweis:

Es ist DHCP-Clients erlaubt die Option "option routers" zu ignorieren.

Um dem vorzubeugen kann die Default-Route inkl. Standard-Gateway an die statischen Routen angehangen werden:

rfc3442-classless-static-routes 16, 188, 144, 192, 168, 230, 73, 15, 100, 102, 17, 10, 192, 168, 230, 73, 0, 192, 168, 230, 10
ms-classless-static-routes 16, 188, 144, 192, 168, 230, 73, 15, 100, 102, 17, 10, 192, 168, 230, 73, 0, 192, 168, 230, 10

Das alles zu scripten ist wirklich Fleisarbeit.

#6 - 2021-09-02 17:03 - flacco

- Due date changed from 2021-01-31 to 2021-12-31

- Target version changed from 14.3 to Future

- % Done changed from 20 to 30

Das Ganze ist deutlich komplexer als gedacht, daher verschoben auf Future.

Die Probleme:

1. Die Syntax der Einträge. Nullen des Netzwerkanteils von IP-Adressen müssen eliminiert werden.
2. Mehrere Routen werden in eine DHCP-Option geschrieben, was vor allem das Hinzufügen von Routen per Script schwierig macht.

Die Vorbereitung für das pushen von Routen ist allerdings bereits im Setup enthalten. Damit können Routen schon manuell im DHCP-Datenbestand im AD eingetragen werden.

#7 - 2021-09-03 16:05 - flacco

- Status changed from New to In Progress