Manuelle und automatisierte Administration einer Active Directory Domäne und Grundlagen der Gruppenrichtlinien

Hannes Schurig

Kaum ein größeres Unternehmen kommt heutzutage noch ohne ein komplexes Computernetzwerk aus. Die Überwachung, Steuerung und Verwaltung eines solchen Netzwerkes erfordert neben dem umfangreichen Fachwissen des verantwortlichen IT-Administrators auch ein elaboriertes Netzwerksystem. In diesem Artikel wird die grundlegende Administration eines Windows Netzwerkes basierend auf einer Active Directory Domäne erklärt und veranschaulicht.

IN DIESEM ARTIKEL ERFAHREN SIE...

- Grundlegendes zu Active Directory Domänen,
- wie Sie mit einem beliebigen Client die Domäne administrieren können,
- · welche Objekte mit welchen Einstellungen enthalten sind,
- welche administrativen Tools zur Vergügung stehen und
- welche Möglichkeiten Gruppenrichtlinien in einer Domäne bieten.

Das Active Directory

Große Computernetzwerke gehören zum Alltag heutiger IT-Administratoren. Diese Netzwerke zu administrieren ist in erster Linie eine Frage der richtigen Technik.

Das Active Directory(oft auch die Kurzform für Active Directory Domain Services– AD DS) ist ein von Microsoft entwickeltes, aus mehreren Diensten bestehendes, zentrales Verwaltungssystem für Windows-Netzwerke. Bei diesem Verwaltungssystem handelt es sich genau genommen um einen hierarchischen Verzeichnisdienst, der Benutzer, Geräte, Freigaben, Einstellungen und vieles mehr gespeichert und administriert werden können.

In Windows Server 2000 kam erstmals das neue Active Directory zum Einsatz und wurde jeweils bei Windows Server 2003 und Windows Server 2008 weiterentwickelt. Es ist somit ein Nachfolger der in Windows NT 4.0 vorhandenen Domänenstruktur, die in ihrer Funktion und Struktur aber sehr eingeschränkt war.

Das Herzstück einer jeden Domäne sind *Domänencontroller* (DC). Diese zentralen Server übernehmen Authentifizierungs- und Autorisierungsprozesse für jedes Objekt und jede Aktion. Sie gewährleisten die Integrität jeder Domäne und sollten bezüglich der Verfügbarkeit und Ausfallsicherheit entsprechend netz- und hardwareseitig ausgestattet werden. Planung, Struktur und Installation eines Domänencontrollers und ei-

WAS SIE VORHER WISSEN SOLLTEN...

• Eine bestehende Active Directory Domäne ist nützlich, weil praxisnahe Tipps jederzeit nachvollzogen werden können.

ner Domäne sind jedoch nicht Gegenstand des Artikels und werden daher nicht weiter vertieft. Microsoft bietet zu diesen Themen ein 6-teiliges Handbuch als kostenlosen PDF-Download^[1].

Administrationstools einrichten

Als zentraler Verzeichnisdienst besteht ein Vorteil von Active Directory darin, von jedem beliebigen Computer



Abbildung 1. Aktivierung der installierten Administrationstools

Anforderungen an Ihren PC:

Die Nutzung von Active Directory Services und somit auch die Administration ist nur mit Windows Betriebssystemen der Edition Professional oder höherwertig möglich.

aus einer Domäne eine vollständige Administration der Domänendienste durchführen zu können.

Um eine komplette Verwaltung aller Aufgaben zu ermöglichen, muss auf dem gewünschten Administrationsclient ein bestimmtes Toolkit installiert werden. Welches Toolkit installiert werden muss, hängt von der Kombinationen aus Serverbetriebssystem (Server 2000, 2003, 2008) und Client (Windows XP, Vista, 7, jeweils Professional oder höherwertig) ab und kann in den von Microsoft zur Verfügung gestellten tabellarischen Übersichten ^{[2][3]} entnommen werden.

Beispielsweise muss bei einem Windows Server 2008 als Serverbetriebssystem und Windows 7 als Clientbetriebs-



Abbildung 2. Benutzerdefinierte Management Konsole mit mehreren Snap-Ins

system das entsprechende *Remoteserver-Administration Toolkit* (RSAT) mit Service Pack 1^[4] installiert werden.

Das Toolkit ist technisch gesehen ein Windows Update und kann auch wie ein solches wieder deinstalliert werden. Alle eingerichteten Funktionen werden dadurch ebenfalls vollständig deinstalliert.

Nach der Installation und einem Neustart müssen die benötigten Verwaltungsprogramme zunächst aktiviert werden.

Dazu genügt es im Menü *Programme und Funktionen-> Windows-Funktionen aktivieren oder deaktivierten*(oder Ausführen -> "optionalfeatures") die gewünschte Punkte auszuwählen und ggf. noch einmal neuzustarten (siehe Abbildung 1).

Hinzugefügte Funktionen erstellen einen Eintrag im "Verwaltung"-Menü von Windows und sind ebenso als Snap-In der *Management Console*(MMC) verfügbar. Die Konsole lässt sich über Ausführen -> "*mmc*" starten.

Es ist empfehlenswert, die MMC mit allen gewünschten Snap-Ins zu versehen, diese zu konfigurieren und die fertige Konsole dann per *Datei-> Speichern unter*schnell und einfach per Doppelklick zugängig zu machen.

Als Beispiel für eine angepasste MMC (siehe Abbildung 2) habe ich die Snap-Ins "Active Directory Schema", "Active Directory-Benutzer und –Computer", "Gruppenrichtlinienverwaltung" und "Richtlinienergebnissatz"

Active Directory-Benutzer und -Computer			x
Datei Aktion Ansicht ?			_
(= -) 2 🗊 🗎 🚍 Q 📑 🛛 🛪	1	7 🗕 🕱	
4 🏥 user.hu-berlin.de	*	usrHUEIQBGroups 265 Objekte	
Builtin			
Computers	_	Name	^
Domain Controllers		SgrUsrHuelqbDruckerSek129	
Foreign SecurityPrincipals		SgrUsrHuelqbDruckerSek239	
LostAndFound		SgrUsrHuelqbDruckerSek244	
Program Data		Souther Street S	
▷ System		Souther Content and Content an	
		Souther Street S	
		Souther Strength & Str	=
		Souther Contract And America Contract And America Amer	-
		& grUsrHuelqbEdvLeitungRW	
		& grUsrHuelqbEdvRW	
usrHUEinrAsa		& grUsrHuelqbEdvSoftwareRW	
⊳ 🛱 usrHUEnrChemie		& grUsrHuelqbEdvVerwRW	
usrHUEinrCMS	Ξ	& grUsrHuelqbEdvWebRW	
IsrHUEinrEthno		Souther the second seco	
IsrHUEinrGBZ		🍇 grUsrHuelqbInstBilderRW	
IsrHUEinrGSZ		🎎 grUsrHuelqbInstCompSoftwRW	
IsrHUEinrIBI		🎎 grUsrHuelqbInstForschDatenRW	
IsrHUEinrIGK		🎎 grUsrHuelqbInstSystem	
usrHUEinrInnovation		🎎 grUsrHuelqbInstVeranstRW	
✓ Image: A state of the sta		🎎 grUsrHuelqbInstVerwRW	
▷ 📴 usrHUEIQBAdm		& grUsrHuelqbPro2AEallgComputerRW	
a usrHUEIQBComputers		& grUsrHuelqbPro2AEallgRW	
USHUEIQBLomputersSoftwareVert		& grUsrHuelqbPro2AEallgVerwRW	
usrHUEIQBComputersSoftware vert Test		& grUsrHuelqbPro2BMIComputerRW	
		& grUsrHuelqbPro2BMImainRW	
b is usrHUFinclAusst		& grUsrHuelqbPro2BMIVeranstRW	
▷ i usrHUEinrMuwi		Souther Street S	
▷ iii usrHUEinrPMK		& grUsrHuelqbPro2DatenserviceRW	
usrHUEinrReha		& grUsrHuelqbPro2DeAbiComputerRW	
usrHUEinrSpowi		& grUsrHuelqbPro2DeAbiRW	
b i usrHUEinrTest	-	🎎 grUsrHuelqbPro2DeAbiVeranstaltungenRW	-
· · · · · · · · · · · · · · · · · · ·			•

Abbildung 3. Hierarchische Domänenstruktur und Namenskonvention



Abbildung 4. Namenskonvention z.B. für Rechtegruppen

Eigenschaften von iqb140	Eigenschaften von 🐲	
Standott Verwaltet von Objekt Sicherheit UNIX-Atribute Atribut-Editor Algemein Betriebssystem Mitglied von Delegierung Kennwortreplikation igb 140 Computername (Prä-Windows 2000): IQB140 DUG Normal DUG Normal	Veröffentlichte Zertfikate Mtgled von Kennwortrepikation Objekt Sicherheit Ungebung Stzungen Remotedesktopdienste-Profil Remotedesktopdienste-Profil Persönlicher vitueller Deskop COM+ UNIX-Attribute Attribut-Editor Algemein Adresse Konto Profil Rufnummem Organisation Image: SuperSide SuperSide SuperSide SuperSide SuperSide SuperSide	Eigenschaften von grUsrHueIqbInstVerwRW
Domänencontrollertyp: Arbeitsstation oder Server Standort: Beschreibung: R411 PRN HP LJ 9050	Vomame: Intialen: Intialen	Gruppenname (Prā-Windows 2000): [rtUstHuelqbInstVerwRW] Beschreibung: Institutsverwaltung E-Mail: Gruppenbereich Gruppentyp () Lokal (in Domäne) () Scherheit
OK Abbrechen Obernehmen Hife	Dubu. Rufnummer: E-Mail: Websete: OK Abbrechen Übernehmen Hilfe	Ciobal Cuhiversal Anmerkung: OK Abbrechen Obernehmen Hife

Abbildung 5. GUIs zur Administration von Objekten

hinzugefügt und konfiguriert. Nach Speichern untersteht mir diese fertige Oberfläche nun jederzeit zur Verfügung.

Aber Achtung: Änderungen an einer Active Directory Domäne werden unwiderruflich umgesetzt, da es keine "*Undo*" Funktion gibt. Vor der Arbeit an einem Produktivsystem sind entsprechende Tests in vorgesehenen Bereichen daher unbedingt notwendig.

Domänenadministration –

Namenskonvention

Ein Blick mit dem Tool "*Active Directory-Benutzer und* –*Computer*" auf größere Domänenstrukturen sollte idealerweise eine gut organisierte Hierarchie mit eindeutigen Namenskonventionen zeigen.

Die Namenskonventionen sollten die hierarchischen Ebenen verdeutlichen, diese sind somit allein aufgrund des Namens in die Struktur exakt einzuordnen.

Ein Beispiel für eine gute Realisierung dieser Standards zeigt folgender Screenshot (siehe Abbildung 3).

Bei der Bennenung von Organisationseinheiten (*Organizational Unit*, OU) - das sind "Container" für weitere Objekte - und Rechtegruppen – genauer gesagt *Sicherheitsgruppen*, mit denen sich NTFS-Berechtigungen setzen lassen und die somit beispielsweise zur riffsrechtedifferenzierung auf Netzlaufwerken dienen - sollte der Name verschiedene relevante Informationen beinhalten.

Ich möchte ein solches Namensschema an einem Beispiel zeigen und beschreiben (siehe Abbildung 4.).

- 1 Kürzel für Rechtegruppen
- 2 Kürzel der Domäne
- 3 Differenzierung der Domäne, z.B. OU-Pfad, hier: Kürzel des Instituts
- 4 Kürzel des Netzlaufwerks
- 5 Kürzel der Ordner und Unterordner
- 6 Rechtetyp (u.A. RO (Read Only), RW (Read Write), FC (Full Control))

Die verständlichen Namen helfen bei der alltäglichen Administration die gewünschten Objekte schneller zu finden.

Domänenadministration – Objekte und Struktur

In der Übersicht von "Active Directory-Benutzer und – Computer" lassen sich die verfügbaren Objekte bereits grundlegend administrieren. Mögliche Objekte sind: Organisationseinheiten, Gruppen, Benutzer, Computer, Kontakte, Drucker und Freigegebene Ordner.

Diese lassen sich dank der grafischen Oberfläche (siehe Abbildung 5) leicht erstellen, bearbeiten, verschieben und löschen. Assistenten helfen sowohl bei komplexeren

Sicherheit Umgebung Sitzungen Remoteüberwachung Remotedesktopdienste-Profil Allgemein Adresse Konto Profil Rufnummern Organisatic Persönlicher virtueller Desktop COM+ UNIX-Attribute Attribut-Edit Attribute:	Veröffentlichte Zertifikate	Mitalie	d von	Kenny	ion Obiel	kt	
Remoteüberwachung Remotedesktopdienste-Profil Allgemein Adresse Konto Profil Rufnummer Organisatic Persönlicher virtueller Desktop COM+ UNIX-Attribute Attribut-Edit Attribute: Attribut Wert IabeledURI IabeledURI <nicht festgelegt=""> IastKnownParent IastLogoff (nie) IastLogon 01.07.2011 10:33:33 IastLogon Nicht festgelegt> IastLogon Some IastLogon Nicht festgelegt> IastLogon Some IastLogon Vicht festgelegt> IastLogon Some IastLogon <nicht festgelegt=""> Iochurt Some IastLogon <nicht festgelegt=""> Iochurt Some IastLogon <nicht festgelegt=""> Iochurt Some IockoutTime <nicht festgelegt=""> Iochurt 683 IogonCount 683 IogonHours <nicht festgelegt=""> IogonWorkstation <nicht festgelegt=""> IogonWorkstation <nicht festgelegt=""></nicht></nicht></nicht></nicht></nicht></nicht></nicht></nicht>	Sicherheit	Umaehung		C			
Allgemein Adresse Konto Profil Rufnummern Organisatic Persönlicher virtueller Desktop COM+ UNIX-Attribute Attribut-Edit Attribute: Attribut Wert Iabeled URI <nicht festgelegt=""> Iabeled URI <nicht festgelegt=""> IastLogoff (nie) IastLogon 01.07.2011 10:33:33 Mitteleuropäische SomilastLogon Timestamp 29.06.2011 17:13:37 Mitteleuropäische Somilegaz/ExchangeDN <nicht festgelegt=""> ImPwdHistory <nicht festgelegt=""> Iockut Time <nicht festgelegt=""> Iockut Time IogonCount 683 IogonWorkstation</nicht></nicht></nicht></nicht></nicht>	Bemeteühenurschun	-		Jizungen			-
Algemein Adresse Norto Profit Nutmummer Organisation Persönlicher virtueller Desktop COM+ UNIX-Attribute Attribut-Edit Attribute:		g Remotedesk			sktopuleriste-Proni		
Attribute: Attribute: Attribute: Iabeled URI Iabeled URI <nicht festgelegt=""> IastLogon 01.07.2011 10:33:33 Mitteleuropäische SomulastLogon IastLogon 01.07.2011 10:33:33 Mitteleuropäische SomulastLogon IastLogon 01.07.2011 11:33:70 Mitteleuropäische SomulastLogon IastLogon <nicht festgelegt=""> IastLogon <nicht festgelegt=""> IocaleID <nicht festgelegt=""> IockoutTime <nicht festgelegt=""> IoginShell <nicht festgelegt=""> IogonCount 683 IogonWorkstation <nicht festgelegt=""></nicht></nicht></nicht></nicht></nicht></nicht></nicht>	Aligemein Aaresse	Konto	Profil	Kurr	ummern	Urganisatio	on
Attribute: Attribut Wert labeledURI <nicht festgelegt=""> lastKnownParent <nicht festgelegt=""> lastLogonf (nie) lastLogon 01.07.2011 10:33:33 Mitteleuropäische SomulastLogon Timestamp 29.06.2011 17:13:37 Mitteleuropäische SomulastLogon Timestamp legacyExchangeDN <nicht festgelegt=""> localeID <nicht festgelegt=""> lockoutTime <nicht festgelegt=""> logonCount 683 logonHours <nicht festgelegt=""> logonWorkstation <nicht festgelegt=""></nicht></nicht></nicht></nicht></nicht></nicht></nicht>	Personlicher virtueller Des	αορ υ	,OM+	UNIX-A	tinbute	Aundul-Euli	.01
Attribut Wert labeledURI <nicht festgelegt=""> lastKnownParent <nicht festgelegt=""> lastLogoff (nie) lastLogon 01.07.2011 10:33:33 Mitteleuropäische SomulastLogon Timestamp legacyExchangeDN <nicht festgelegt=""> localeID <nicht festgelegt=""> lockoutTime <nicht festgelegt=""> logonCount 683 logonHours <nicht festgelegt=""> logonWorkstation <nicht festgelegt=""></nicht></nicht></nicht></nicht></nicht></nicht></nicht>	Attribute:						
labeledURI <nicht festgelegt=""> lastKnownParent <nicht festgelegt=""> lastLogoff (nie) lastLogon 01.07.2011 10:33:33 Mitteleuropäische SomulastLogon Timestamp lastLogon Timestamp 29.06.2011 17:13:37 Mitteleuropäische SomulastLogon Timestamp legacyExchangeDN <nicht festgelegt=""> ImPwdHistory <nicht festgelegt=""> localeID <nicht festgelegt=""> lockoutTime <nicht festgelegt=""> logonCount 683 logonHours <nicht festgelegt=""> logonWorkstation <nicht festgelegt=""></nicht></nicht></nicht></nicht></nicht></nicht></nicht></nicht>	Attribut	Wert				•	
lastKnownParent <nicht festgelegt=""> lastLogoff (nie) lastLogon 01.07.2011 10:33:33 Mitteleuropäische SomulastLogon Timestamp lastLogon Timestamp 29.06.2011 17:13:37 Mitteleuropäische SomulastLogon Timestamp legacyExchangeDN <nicht festgelegt=""> lmPwdHistory <nicht festgelegt=""> localeID <nicht festgelegt=""> lockoutTime <nicht festgelegt=""> logonCount 683 logonHours <nicht festgelegt=""> logonWorkstation <nicht festgelegt=""></nicht></nicht></nicht></nicht></nicht></nicht></nicht>	labeledURI	<nicht fee<="" td=""><td>stgelegt></td><td></td><td></td><td></td><td></td></nicht>	stgelegt>				
lastLogoff (nie) lastLogon 01.07.2011 10:33:33 Mitteleuropäische SomulastLogon Timestamp lastLogon Timestamp 29.06.2011 17:13:37 Mitteleuropäische SomulastLogon Timestamp legacyExchangeDN <nicht festgelegt=""> lmPwdHistory <nicht festgelegt=""> localeID <nicht festgelegt=""> lockoutTime <nicht festgelegt=""> logonCount 683 logonHours <nicht festgelegt=""> logonWorkstation <nicht festgelegt=""></nicht></nicht></nicht></nicht></nicht></nicht>	last Known Parent	<nicht fee<="" td=""><td>stgelegt></td><td></td><td></td><td></td><td></td></nicht>	stgelegt>				
lastLogon 01.07.2011 10:33:33 Mitteleuropäische SomulastLogon Timestamp lastLogon Timestamp 29.06.2011 17:13:37 Mitteleuropäische SomulegacyExchangeDN legacyExchangeDN <nicht festgelegt=""> lmPwdHistory <nicht festgelegt=""> localeID <nicht festgelegt=""> lockoutTime <nicht festgelegt=""> loginShell <nicht festgelegt=""> logonCount 683 logonHours <nicht festgelegt=""> logonWorkstation <nicht festgelegt=""></nicht></nicht></nicht></nicht></nicht></nicht></nicht>	lastLogoff	(nie)					
lastLogonTimestamp 29.06.2011 17:13:37 Mitteleuropäische Somi legacyExchangeDN <nicht festgelegt=""> ImPwdHistory <nicht festgelegt=""> localeID <nicht festgelegt=""> lockoutTime <nicht festgelegt=""> loginShell <nicht festgelegt=""> logonCount 683 logonHours <nicht festgelegt=""></nicht></nicht></nicht></nicht></nicht></nicht>	lastLogon	01.07.20	11 10:33:3	3 Mittel	europäisch	ne Som	
legacyExchangeDN <nicht festgelegt=""> ImPwdHistory <nicht festgelegt=""> localeID <nicht festgelegt=""> lockoutTime <nicht festgelegt=""> loginShell <nicht festgelegt=""> logonCount 683 logonHours <nicht festgelegt=""></nicht></nicht></nicht></nicht></nicht></nicht>	lastLogon Timestamp	29.06.20	11 17:13:3	7 Mittel	europäisch	ne Somi	
ImPwdHistory <nicht festgelegt=""> localeID <nicht festgelegt=""> lockoutTime <nicht festgelegt=""> loginShell <nicht festgelegt=""> logonCount 683 logonHours <nicht festgelegt=""> logonWorkstation <nicht festgelegt=""></nicht></nicht></nicht></nicht></nicht></nicht>	legacyExchangeDN	<nicht fes<="" td=""><td>stgelegt></td><td></td><td></td><td></td><td></td></nicht>	stgelegt>				
localeID <nicht festgelegt=""> lockoutTime <nicht festgelegt=""> loginShell <nicht festgelegt=""> logonCount 683 logonHours <nicht festgelegt=""> logonWorkstation <nicht festgelegt=""></nicht></nicht></nicht></nicht></nicht>	ImPwdHistory	<nicht fes<="" td=""><td>stgelegt></td><td></td><td></td><td></td><td></td></nicht>	stgelegt>				
lockoutTime <nicht festgelegt=""> loginShell <nicht festgelegt=""> logonCount 683 logonHours <nicht festgelegt=""> logonWorkstation <nicht festgelegt=""></nicht></nicht></nicht></nicht>	localeID	<nicht fes<="" td=""><td>stgelegt></td><td></td><td></td><td></td><td></td></nicht>	stgelegt>				
loginShell <nicht festgelegt=""> logonCount 683 logonHours <nicht festgelegt=""> logonWorkstation <nicht festgelegt=""></nicht></nicht></nicht>	lockoutTime	<nicht fe<="" td=""><td>staeleat></td><td></td><td></td><td></td><td></td></nicht>	staeleat>				
logonCount 683 logonHours <nicht festgelegt=""> logonWorkstation <nicht festgelegt=""></nicht></nicht>	loginShell	<nicht fe<="" td=""><td>staeleat></td><td></td><td></td><td></td><td></td></nicht>	staeleat>				
logonHours <nicht festgelegt=""> logonWorkstation <nicht festgelegt=""></nicht></nicht>	logonCount	683					
logonWorkstation <nicht festgelegt=""></nicht>	logonHours	<nicht fe<="" td=""><td>staeleat></td><td></td><td></td><td></td><td></td></nicht>	staeleat>				
	logonWorkstation	<nicht fe<="" td=""><td>staeleat></td><td></td><td></td><td></td><td></td></nicht>	staeleat>				
mail <nicht festgelegt=""></nicht>	mail	<nicht fe<="" td=""><td>staeleat></td><td></td><td></td><td>-</td><td></td></nicht>	staeleat>			-	
۲ III ۲						P.	
Bearbeiten	Bearbeiten					Filter	

Abbildung 6. Erweiterter Attribut-Editor

Vorgängen wie die Erstellung von Objekten als auch bei anderen Konntextmenü-Aktionen (Export, Import usw.).

Das Tool "Active Directory-Benutzer und –Computer" bietet auch "erweiterte Features". Diese werden über Ansicht-> erweiterte Featuresaktiviert.

Erwähnenswert ist beispielsweise der erweiterte Attribut-Editor (siehe Abb. 6), der nach der Aktivierung als zusätzlicher Tab bei den Objekten verfügbar ist. Dieser enthält alle für das Objekt verfügbaren Eigenschaften des Active Directory Schemas.

Aber Achtung: Änderungen an dieser Stelle können unter Umständen erhebliche Schäden verursachen und sollten nur mit Bedacht und Fachkenntnis vorgenommen werden.

Grafische Darstellung der Domänenstruktur:

Die Struktur einer Domäne nimmt mit zunehmender Größe auch an Unübersichtlichkeit zu. Die MMC Snap-In Übersichten bieten eine gute Grundlage. Für einen alternativen Überblick, Grafiken, Statistiken oder Reports empfehle ich jedoch externe Tools. Zum Beispiel das kostenlosen Tool "Jose AD-Dokumentation"^{[5][6]} von Nils Kaczenski. Es fertigt stark anpassbare und übersichtliche HTML Reports von Domänenstrukturen an.

Eine weitere Möglichkeit der grafischen Darstellung bietet der *Microsoft Active Directory Topology Diagrammar*(MS ADTD). Dieser erstellt eine Visio-fähige 2D-Shape-Grafik (siehe Abbildung 7), in der die Struktur der Server, Domänen, Sites und OUs grafisch dargestellt wird^[7].

Domänenadministration – automatisierte Administration

Für einzelne Aktionen ist die grafische Oberfläche meistens besser geeignet; bei Massenaktionen und –abfragen ist eine automatisierte Lösung jedoch unverzichtbar.

Abfragen mit CSVDE:

Das Konsolenprogramm csvde.exe von Microsoft wurde entwickelt, um Daten aus einem Active Directory zu im- oder exportieren.



Abbildung 7. Grafische Darstellung der Domänen-Server-Struktur mit MS ADTD

Wie der Name schon andeutet, arbeitet das Programm mit CSV-Dateien, (*Comma-Separated Values*) die wiederum von Excel oder Calc betrachtet und verarbeitet werden können.

Das Tool ist in den Betriebssystemen Windows Server 2003 und 2008 integriert und liegt in *%windir%\system32*. Alternativ ist es im installierbaren Paket *"Active Directory Application Mode"^[8]* (ADAM, z.B. für Windows XP) enthalten.

Die ausführliche Beschreibung der Parameter und Nutzungshinweise stehen im Microsoft TechNet^[9] zur Verfügung; ich möchte an dieser Stelle nur einen Befehl exemplarisch zeigen und erklären (siehe Listing 1.).

Dieser Befehl liest alle Computerobjekte der OU *usrHUEinrIQB*aus und schreibt sie mitsamt einiger Eigenschaften in eine CSV Datei (siehe Abbildung 8). Hier eine etwas genauere Aufschlüsselung des Befehls:

- m überspringt einige spezielle Attribute
- n überspringt Binärwerte
- u erzwingt das Unicodeformat f
 ür korrekte Umlaute
- f bestimmt die Ausgabedatei
- s bestimmt einen gezielten Domänencontroller
- d bestimmt die Datenquelle
- r bestimmt den LDAP Suchfilter und Achtung: objectClass=user & objectCategory=computer

Listing 1. CSVDE Abfrage der Computerobjekte einer OU

exportiert nur die Computer, objectClass=user & objectClategory=person nur die Benutzer.

• I enthält alle gewünschten LDAP Attribute. Diese sind im Internet nachlesbar^{[10][11]}.

Abfragen mit PowerShell:

Die PowerShell ist eine in Windows Server 2008 erstmals eingeführte Befehlszeilenumgebung, die mit der klassischen Kommandozeile aus Windows (CMD) vergleichbar ist. PowerShell bietet jedoch eine stark überarbeitete und strukturiertere Scriptsprache, die sich durch Plugins mit vielen weiteren Funktionen nachrüsten lässt.

In Windows Server und Windows 7 muss die PowerShell zuerst aktiviert werden. Auf dem Server erfolgt das über den Server-Manager -> Features oder über den CMD Befehl servermanagercmd -install powershell. In Windows 7 muss das Feature in den Windows Features (Ausführen -> "optionalfeatures") aktiviert werden. Für Windows XP und Windows Vista gibt es das Windows Management-Framework (WMF), das u.A. auch PowerShell in der neueren Version 2.0 beinhaltet^[12]. Alternativ zu diesem Download liefert das WMF Core Package ohne BITS^[13] auch alle nötigen Komponenten mit.

Die Installationen enthalten sogar eine Entwicklungsumgebung namens PowerShell ISE (PowerShell In-

```
csvde -m -n -u -f "computersummary.csv" -s dcserver -d "OU=usrHUEinrIQB,OU=usrHUEinr,DC=domain,DC=corporati
on,DC=com" -r "(|(&(objectClass=user) (objectCategory=computer)))" -l name, description,
operatingsystem, operatingsystemversion, operatingsystemservicepack, modifyTimeStamp
```

Listing 2. PowerShell Abfrage der Computerobjekte mit Filter und Sortierung

```
function GetComputersFromLDAP() {
   pcs = 0();
   $dir = "LDAP://OU=usrHUEIQBComputers,OU=usrHUEinrIQB,OU=usrHUEinr,DC=user,DC=hu-berlin,DC=de";
   $ldapSearcher = new-object directoryservices.directorysearcher;
   $ldapSearcher.filter = ``(objectclass=computer)";
   $computers = $ldapSearcher.findall();
   foreach ($computer in $computers) {
      if ($computer.properties["operatingsystem"] -eq "Windows 7 Enterprise N") {
          $pc = ``'' | select-object Name;
          $pc.Name = $computer.properties["name"];
          $pcs += $pc;
      ł
   3
   return ($pcs | sort-object Name);
}
foreach ($pc in $pcs) {
    write-host $pc.Name;
ł
GetComputersFromLDAP("");
```


tegrated Scripting Environment), die neben üblichen Bearbeitungsfunktionen auch das Debuggen von PowerShell Scripts beinhaltet.

Solche Scripts werden mit der Dateiendung .ps1angelegt und können über die PowerShell Befehlszeile, mit *Rechtsklick-> Mit PowerShell ausführen*oder über das ISE ausgeführt werden.

Wenn die Ausführung fehlschlägt, kann das an der gesetzen Ausführungsrichtlinie (*Execution Policy*) des Computers liegen, die in der Standardeinstellung so eingestellt ist, dass keine Scripte ausgeführt werden dürfen.

Mit dem Befehl Set-ExecutionPolicy unrestricted wird die Ausführung jeglicher PowerShell Scripte auf diesem System gewährt.

Aber Achtung: Die Ausführungsrichtlinie sollte nicht leichtfertig gesetzt werden, da sie ein Sicherheitsrisiko darstellt. Mehr Informationen zur Execution Policy im Internet^[14].

Nun zeige ich ein Script^[15], das die Computer einer Domäne ausliest und alle Computer – nach Namen sortiert - anzeigt, die das Betriebssystem *"Windows 7 Enterprise N"* installiert haben.

Gruppenrichtlinien – Überblick

Mit den Gruppenrichtlinien hat Microsoft ein mächtiges Werkzeug entwickelt, um beliebig viele Computer eines Netzwerks von einer zentralen Administrationsstelle aus mit Einstellungen und Programmen zu versehen.

Gruppenrichtlinien können sich auf einzelne Objekte, Gruppen oder ganze Domänen auswirken und ermöglichen damit unternehmensweite automatisierte Administration auf Computer- oder Benutzerebene.

Viele Einstellungen werden jeweils in einem Gruppenrichtlinienobjekt (*Group Policy Object*, GPO) zusammengefasst. Dieses wird nun mit einem Container des Active Directory verknüpft. Meistens sind das einzelne OUs, es können aber auch ganze Sites oder Domänen verknüpft werden. Ein Gruppenrichtlinienobjekt kann mit beliebig vielen Containern verknüpft sein, ebenso kann ein Container beliebig viele GPOs enthalten.

Gruppenrichtlinien können recht einfach über das grafische MMC Snap-In Gruppenrichtlinienverwaltung" verwaltet werden (siehe Abbildung 9).

Die Oberfläche dieses Programms ähnelt dem Aufbau der Domänenverwaltung. Statt Benutzer, Computer

Microsoft Excel - computers.csv	
Date Bearbeiten Ansicht Einfügen Format Extras Dater Adgbe PDF Frage hier eingebe	n - ∎×
🗋 🖆 🛃 👌 🖤 🎎 & 🛍 • 의 • 🌆 🧶 Σ • 🔄 🏨 100% • 🞯 🚆 10 • F K 🖳 票 署 🧮 尾 🖽 • 💩 • 📥 •	🛛 🗄 📩 🛒 🖕
A1 AD DN, description, name, modifyTimeStamp, operatingSystem, operatingSystemVersion, operatingSystemServicePack	
H I J K L M N O P Q R S	т —
25 bB,OU=usrHUEinr, 2010 R404 R404 R404 R404 R404 R404 R404 R	^
26 \B,OU=usrHUEinr, 24 a 26 \B,OU=usrHUEinr, 26 26 \B,OU=usrHUEi	
27 JB,OU=usrHUEinr States of the R233 results	
28 DB OU=usrHUE int (2000) R408 K 2000 (2000) R408 K 2000 (2000) R408 K 2000) R408 K 2000 (2000) R408 K 2000 (2000) R408 K 2000) R408 K 2000 (2000) R408 K 2000) R408 K 2000 (2000) R408 K 2000) R408 K 2000 (2000) R408 K 2000) R408 K 2000 (2000) R	
29 bp.00=usrMUEinr, Charles Annual C	=
31 bB OLD-darin Delm, and a start and a st	
2 DB OL=usrHUE int 2 + + + + + + + + + + + + + + + + + +	
33 DB OU=usrHUEinr. 4 + + + + + + + + + + + + + + + + + +	
34 DB,OU=usrHUEinr, 2010 A Contract of the second s	
35 B.OU=usrHUEinr, 34 34 34 34 34 34 34 34 34 34 35 36 36 37 36 37 36 38 38 38 38 38 38 38 38 38 38 38 38 38	
36 2B,OU=usrHUEinr, 2010 2010 2010 2010 2010 2010 2010 201	
37 PB,OU=usrHUEinr, 2010 And 201	
38 BP.OU=usrHUEinr, A. S.	
39 Db. OU=usrHUEInf, as a set of the set of	
40 bp.00-usinibusini sector and a sector and	
42 DB OLl=usrHI/Einr 2010 1000 1100 1100 1100 1100 1000 11000 1100	
43 DB OU=usrHUEinr. R135 F R13	
44 DB.OU=usrHUEinr, 2010 10 10 10 10 10 10 10 10 10 10 10 10	
if (+) h computers/	► a
Bereit	VF
	My Drophox
Historest Histores (Statements)	Hy Diopbox
Copyright Cc) 2009 Microsoft Corporation. Alle Rechte vorbehalten.	Erw. Grö
x:\Software\Sustem\Scripte>csude -m -n -u -f "computers.csu" -s 👾 🖓 👘 -d "OU=	<d'< td=""></d'<>
usrHUEinrIQB, ÓU=usrHUEinr, 💥 🐲 🐨 🐨 🐨 🐨 👘 👘 🕂 🕂 ({{&(objectClass=user)	csv 5
Vojectategory-computer/// -1 name_description.operatingsystem.operatingsystem	wsf
CreateIQBComputerAccount_template	bat
Create lugbuser	bat
v:\Softwave\Sustem\Sevinte>	exe 3
S get Multiple Users For OU	wsf 1
📓 🛃 🛃 🛃 🛃 🛃 🛃 🛃 🛃 🛃 🛃	
	wsf
get UserInfo	wsf bat
get Userinfo	wsf bat wsf
get UserInfo get UserInfo HistoryCreateComputerAccounts HistoryCreateUser	wsf bat wsf txt txt
Get UserInfo get UserInfo HistoryCreateComputerAccounts HistoryCreateUser HistoryCreateUser	wsf bat wsf txt txt
Get UserInfo get UserInfo Jet UserInfo HistoryCreateComputerAccounts HistoryCreateUser	wsf bat wsf txt txt

Abbildung 8. Datenabfrage der Domäne mit csvde

Im Internet

- [1] http://bit.ly/pV2J16 "Active Directory: Das Planungshandbuch"
- [2] http://support.microsoft.com/kb/304718 Übersicht: Administration Toolkits
- [3] http://support.microsoft.com/kb/958830 Übersicht: Administration Toolkits
- [4] *http://bit.ly/ilrfWd* RSAT mit SP1 für Windows 7
- [5] http://bit.ly/oJLQic José AD-Dokumentation 3.1
- [6] http://bit.ly/e99OSg Hilfe, FAQ, Tipps, Code
- [7] http://bit.ly/nLWFGi MS ADTD Artikel
- [8] http://bit.ly/nZOmb2 Active Directory Application Mode mit csvde
- [9] http://bit.ly/ogyFqs Dokumentation zu csvde.exe
- [10] http://www.selfadsi.de/user-attributes-w2k3.htm LDAP Attribute grafisch
- [11] http://bit.ly/pPw7Sa LDAP Attribute als Text
- [12] http://support.microsoft.com/kb/968929 Windows Management-Framework
- [13] http://support.microsoft.com/kb/968930 Windows Management-Framework Core
- [14] http://bit.ly/qox3zw Informationen zur ExecutionPolicy
- [15] http://bit.ly/rnMX9D Codebeispiel PowerShell Abfrage
- [16] http://bit.ly/aKf8fn Troubleshooting von Gruppenrichtlinien
- [17] http://bit.ly/pY4hpb Zahlen zu Gruppenrichtlinieneinstellungen

Lange Links werden für eine bessere Übersicht mit www.bit.ly gekürzt.

Zusätzliche Quellen

Eric Tierling: Windows Server 2008. Einrichtung, Verwaltung, Referenz. München: Addison-Wesley Verlag, 2009 Ulrich Schlüter: Integrationshandbuch Microsoft Netzwerk. 3. akt. und erw. Aufl. Bonn: Galileo Press

oder andere Objekte werden hier allerdings die GPOs in den einzelnen OUs gezeigt.

Im Kontextmenü eines Richtlinienobjekts stehen weitere Funktionen wie die Sicherung so wie Wiederherstellung, der Status als auch ein Richtlinienbericht zur Verfügung.

Bei Problemen mit Gruppenrichtlinien hilft meist ein solcher Gruppenrichtlinienbericht vom Client. Dieser wird über das "Richtlinienbericht" Snap-In oder mit dem Befehl gpresult in der Kommandozeile erstellt. Weitere Hinweise zur Problembehebung bieten die Protokolle der Ereignisanzeige (ebenfalls auf den Clients) oder ein kritischer Blick über die vielen Einstellungsmöglichkeiten und Rechte der Gruppenrichtlinie^[16].

Gruppenrichtlinien – Einstellungen

Fast alle Einstellungen der Gruppenrichtlinien manipulieren letzten Endes die Registry des Clients und wer-



Abbildung 9. Einstellungen in der Gruppenrichtlinienverwaltung

den dadurch wirksam. Mit der neuesten Servertechnologie (Windows Server 2008 R2) existieren weit über 3.000 Gruppenrichtlinieneinstellungen, die auf dem Client über 11.000 Registrywerte manipulieren können^[17].

Um eine bessere Struktur und logische Übersicht zu schaffen, sind die Einstellungen der GPOs in 2 Bereiche aufgeteilt: *Computerkonfiguration Benutzerskonfiguration*. Das Verhalten dieser Einstellungen ist leicht unterschiedlich: Computereinstellungen werden beim Systemstart noch vor der Anmeldung des Benutzers angewendet. Benutzereinstellungen werden im Gegensatz dazu erst nach der Anmeldung übernommen, wenn diesem Benutzer oder einer Gruppe, in der dieser Benutzer Mitglied ist, Einstellungen über die Benutzerkonfiguration zur Verfügung gestellt worden sind.

Dank dieser Gruppenrichtlinieneinstellungen lassen sich viele Bereiche des Windowssystems, unabhängig von der Größe des Netzwerks, homogen gestalten und verwalten. Der Aufwand ist durch die einmalige Konfiguration am Server minimal.

HANNES SCHURIG

Der Autor ist IT-Administrator in einem wissenschaftlichen Institut mit den Schwerpunkten Netzwerk- und Serveradministration. Privat beschäftigt er sich seit vielen Jahren mit Windows Systemen, deren Administration und verschiedenen Bereichen der Webentwicklung und Webdesign.

Er ist Betreiber des privaten Blogs www.hannes-schurig.de, in dem er regelmäßig über diese Themen schreibt.

Privat: hannes.schurig@online.de

Blog: kontakt@hannes-schurig.de