Quelle: Olga Yastremska – 123RF

Objekte und deren Attribute im Active Directory sichern und wiederherstellen

Sorgenfrei

von Dr. Christian Knermann

Schnell ist es passiert: Sie haben versehentlich Objekte im Active Directory gelöscht oder deren Attribute verändert. Mit kostenlosen Hilfsmitteln von Microsoft und etwas Vorbereitung sorgt eine solche Situation nicht mehr für erhöhten Puls. IT-Administrator zeigt, wie Sie sich rüsten und verlorene Informationen wiederherstellen.

Wer sich mit der Sicherung und Wiederherstellung von Windows Servern sowie Gesamtstrukturen und Domänen im Active Directory (AD) beschäftigt, stößt zuerst auf die Bordmittel [1]. Das im Betriebssystem enthaltene Feature "Windows-Server-Sicherung" erstellt Backups von Domänencontrollern (DC) mitsamt Systemstatus. Letzterer schließt das AD zum Zeitpunkt der Sicherung mit ein und beugt damit den großen Katastrophen vor. Alternativ helfen hierbei auch Drittanbietertools, wie etwa "U-Move for Active Directory" (Testbericht ab Seite 24 in dieser Ausgabe).

Autoritatives und nicht-autoritatives Restore

Fällt nur ein einzelner DC aus, während weitere noch über ein intaktes AD verfügen, holt eine nicht-autoritative Wiederherstellung das ausgefallene System aus der Windows-Server-Sicherung zurück. Als nicht-autoritativ bezeichnet Microsoft diesen Fall, da sich der restaurierte DC den anderen unterordnet. Im Backup noch vorhandene AD-Objekte, die zwischenzeitlich gelöscht wurden, verschwinden auf dem wiederhergestellten DC, da er den aktuellen Status des ADs von den übrigen Controllern repliziert.

Eine autoritative Wiederherstellung holt dagegen einen DC einschließlich Zustand des ADs aus dem Backup zurück. In diesem Fall übernimmt das wiederhergestellte System die Führung und überschreibt das AD auf eventuell noch vorhandenen weiteren Controllern. Die autoritative Wiederherstellung ist somit der Rettungsanker bei Totalverlust oder Beschädigung einer AD-Gesamtstruktur. Das Verfahren eignet sich ebenso für die kleinen Katastrophen des Alltags. Es holt einzelne gelöschte oder veränderte Objekte aus einem Systemstatus-Backup zurück, ist aber komplex in der Anwendung [2]. Doch glücklicherweise geht es auch einfacher.

AD-Papierkorb aktivieren

Bereits mit Windows Server 2008 R2 führte Microsoft einen Papierkorb für das AD ein. Dieser hilft Ihnen dabei, versehentlich gelöschte Objekte zu restaurieren, ohne den umständlichen Weg über eine autoritative Wiederherstellung zu bemühen. Allerdings ist der Papierkorb auch in aktuellen Ausgaben des Windows Servers ab Werk nicht eingeschaltet.

Damit Sie ihn aktivieren können, muss die Funktionsebene Ihrer AD-Gesamtstruktur mindestens Windows Server 2008 R2 entsprechen. Sollte dies noch nicht der Fall sein, verwenden Sie die Konsole "Active Directory-Domänen und -Vertrauensstellungen", um die Gesamtstrukturfunktionsebene und am besten auch gleich die Domänenfunktionsebene heraufzustufen. Dieser Vorgang ist jedoch nur schwer wieder rückgängig zu machen und das nun folgende Aktivieren des Papierkorbs sogar irreversibel.

Im Folgenden gehen wir exemplarisch von einer AD-Gesamtstruktur mit nur einer Domäne namens "itablog.local" aus. Ersetzen Sie diesen Namen sowie den Teilstring "DC=itablog, DC=local" durch für Ihre Umgebung zutreffende Werte. Anfangs war es nur per PowerShell möglich, den Papierkorb zu aktivieren. Melden Sie sich entsprechend mit einem Benutzerkonto, das Mitglied der Gruppe "Organisations-Admins" ist, an dem DC an, der die FSMO-Rolle "Domain Naming Master" hält, und führen Sie das folgende Kommando aus:

```
Enable-ADOptionalFeature -Identity
  'CN=Recycle Bin Feature, CN=Optio-
  nal Features, CN=Directory Ser-
  vice, CN=Windows NT, CN=Services,
  CN=Configuration, DC=itablog,
  DC=local' -Scope ForestOrConfigu-
  rationSet -Target 'itablog.local'
```

Ab Windows Server 2012 aufwärts schalten Sie den Papierkorb alternativ auch grafisch über das Active-Directory-Verwaltungscenter ein. Markieren Sie dazu links in der Navigationsleiste Ihre Gesamtstruktur und führen Sie dann rechts bei den Aufgaben die Aktion "Papierkorb aktivieren…" aus. Warten Sie anschließend, bis alle DCs die Änderung repliziert haben. Sobald Sie das AD-Verwaltungscenter neu starten, erscheint in der Ansicht Ihrer Gesamtstruktur der neue Container "Deleted Objects". Alle AD-Objekte, die Sie von nun an löschen, landen in diesem Container. Das gilt für

Benutzer, Computer, Gruppen und auch für ganze Organisationseinheiten (Organizational Unit, OU).

Löschfristen beachten

Doch Obacht, die Objekte bleiben im Papierkorb nicht ewig erhalten. Wann das Active Directory die gelöschten Objekte aufräumt, richtet sich nach zwei Fristen, der Deleted Object Lifetime (DOL) und der Tombstone Lifetime (TSL). Beides sind Eigenschaften auf Ebene der Gesamtstruktur [3] der Umgebung.

Das Wichtigste in aller Kürze: Nur innerhalb der DOL können Sie ein Objekt wiederherstellen und standardmäßig setzt Windows die DOL gleich der TSL. Wie lange der in Tagen bemessene Zeitraum tatsächlich ist, hängt von der Vorgeschichte Ihrer AD-Gesamtstruktur ab. In einer Umgebung, die auf den Windows Server 2003 SP1 oder einen seiner Nachfolger zurückgeht, beträgt die TSL 180 Tage. Reicht der Migrationshintergrund Ihres ADs jedoch bis zum Windows Server 2003 ohne Service Pack oder seinem Vorfahren zurück, beträgt die TSL nur 60 Tage.

Möchten Sie die Werte anpassen, hilft Ihnen der ADSI-Editor (Bild 1) oder wiederum die PowerShell. Exemplarisch konfigurieren die beiden folgenden Kommandos 365 Tage für die DOL und 180 Tage für die TSL:

```
Set-ADObject -Identity "CN=Directory
  Service, CN=Windows NT, CN=Ser-
  vices, CN=Configuration, DC=itab-
  log, DC=local" -Partition "CN=Con-
  figuration, DC=itablog, DC=local"
  -Replace:@{"msDS-DeletedObjectLi-
  fetime" = 365}

Set-ADObject -Identity "CN=Directory
  Service, CN=Windows NT, CN=Services,
  CN=Configuration, DC=itablog, DC=lo-
  cal" -Partition "CN=Configuration,
  DC=itablog, DC=local" -Replace:@
  {"tombstoneLifetime" = 180}
```

Objekte aus dem Papierkorb wiederherstellen

Auch beim Wiederherstellen von Objekten dürfen Sie zwischen der PowerShell und der grafischen Anzeige wählen. Mittels

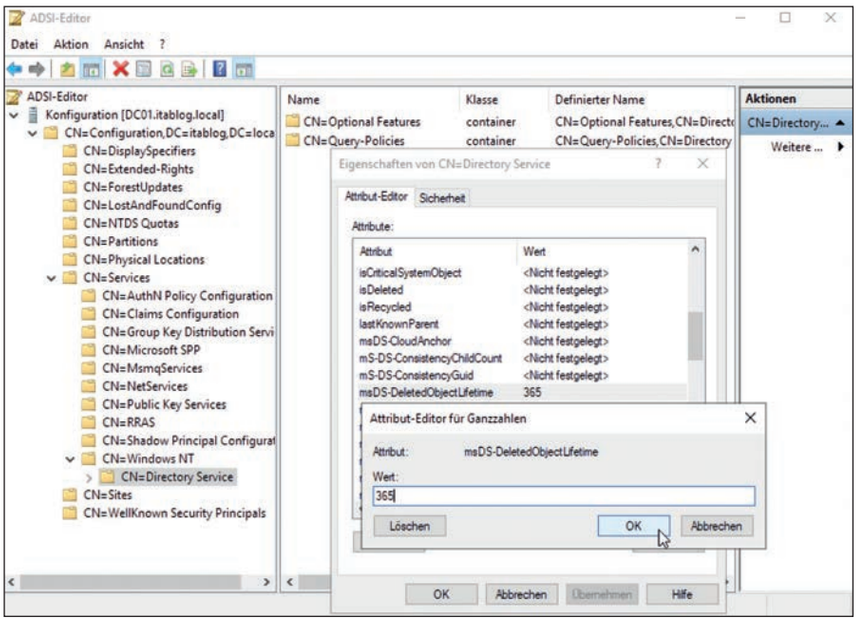

Bild 1: Die Deleted Object Lifetime (DOL) legt fest, wie lange der AD-Papierkorb gelöschte Objekte aufbewahrt.

```
Get-ADObject -filter 'isdeleted -eq
  $true -and name -ne "Deleted Ob-
  jects"' -includeDeletedObjects
  -property *
```

verschaffen Sie sich einen detaillierten Überblick über den Inhalt des Papierkorbs. Haben Sie etwa versehentlich ein Benutzerkonto mit dem Anzeigenamen "Ahner, Paul" gelöscht, holen Sie das Konto mit dem folgenden Befehl aus dem Papierkorb zurück:

```
Get-ADObject -Filter {displayName
  -eq "Ahner, Paul"} -IncludeDele-
  tedObjects | Restore-ADObject
```

Dasselbe erreichen Sie, indem Sie das gelöschte Objekt im Container "Deleted Objects" des AD-Verwaltungscenters markieren und rechts aus der Aufgabenliste "Wiederherstellen" wählen. Mittels "Wiederherstellen in…" restaurieren Sie das Objekt alternativ in eine andere OU als die, in der es sich ursprünglich befunden hat (Bild 2). Das ist praktisch, wenn Sie nicht nur ein Objekt, sondern auch seine übergeordnete OU gelöscht haben: Ohne Weiteres ist es nämlich nicht möglich, verschachtelte Strukturen gelöschter Objekte in einer einzelnen Aktion zurückzuholen.

Möchten Sie eine OU mit all ihren Unter-OUs und darin enthaltenen Objekten wiederherstellen, erläutert Microsoft das manuelle Vorgehen mittels AD-Verwaltungscenter [4] und verweist auch auf ein nützliches PowerShell-Skript [5]. Das Skript geht zwar noch auf Server 2008 R2 zurück, leistet aber auch unter aktuellen Versionen des Betriebssystems noch gute Dienste.

Speichern Sie das Skript lokal als "Restore-ADTree.ps1". Haben Sie nun versehentlich die OU mit dem Distinguished Name "OU=Marketing, OU=Benutzer, DC=itablog, DC=local" und alle Benutzer darin ins Jenseits befördert, holt eines der beiden Kommandos

```
.\Restore-ADTree.ps1 -lastKnownRDN
  Marketing

.\Restore-ADTree.ps1 -identity
  "OU=Benutzer,DC=itablog,DC=local"
```

alle betroffenen Objekte in Windeseile zurück, als wäre nichts geschehen. Der AD-Papierkorb ist damit eine äußerst praktische Ergänzung zu einer Systemstatussicherung, aber kein Ersatz dafür. Der Papierkorb hilft nicht, wenn das AD als Ganzes Schaden genommen hat. Weiterhin holt der Papierkorb nur komplett gelöschte Objekte zurück. Doch was, wenn Sie ein oder mehrere Objekte nicht gelöscht, sondern versehentlich nur einzelne ihrer Attribute verändert haben?

Snapshots per PowerShell

Intern handelt es sich beim AD um eine Datenbank, gespeichert in der NTDS.DIT-Datei, die Sie standardmäßig im Pfad "%systemroot%\NTDS" finden. Liegt sie nicht dort, verrät Ihnen der Registry-Schlüssel "HKLM \ SYSTEM \ CurrentControlSet \ Services \ NTDS \ Parameters \ DSA Database file" den richtigen Ort.

Schon seit Windows Server 2008 bietet Microsoft die Möglichkeit, mittels des Volume Shadow Copy Service (VSS) beliebig viele Snapshots der Datenbank zu erzeugen und auf die in den Snapshots enthaltenen Versionsstände zurückzugreifen. Grenzen setzt dem lediglich der zur Verfügung stehende Festplattenplatz. Die AD-Snapshots erfordern allerdings die Kommandozeilenwerkzeuge Ntdsutil sowie Dsamain und sind nicht gerade intuitiv in der Anwendung.

Praktischerweise hat der ehemalige Microsoft-Mitarbeiter und PowerShell-Spezialist Ashley McGlone die Bordmittel um einige PowerShell-Cmdlets erweitert und diese in Form des Skripts "AD_Snapshot_Functions.ps1" kostenlos veröffentlicht. Das Skript funktioniert von Haus aus allerdings nur auf einem englischsprachigen System. Der Grund hierfür ist, dass das Cmdlet zum Mounten eines Snapshots die Rückgabe des Befehls Ntdsutil auswertet und eine Antwort der Form "Snapshot ... mounted as C:\$SNAP_..._VOLUMEC$\" erwartet. Ist die Systemsprache Deutsch, gibt Ntdsutil jedoch "Der Snapshot ... wird als C:\$SNAP_..._VOLUMEC$\ bereitgestellt." zurück.

Damit das Skript funktioniert, ohne ein englisches Sprachpaket zu installieren und zum Standard zu erklären, tauschen wir die Zeile 167 des Skripts gegen den folgenden Code aus:

```
$MountPath = (($Mount | Select-
  String -SimpleMatch 'wird als' |
  Where-Object {$_ -like
  "*VOLUME$($DITPathDrive)$*"})
  -split 'wird als')[-1].Trim().
  TrimEnd(" bereitgestellt.")
```

Die fertigen Skripte für beide Sprachen finden Sie unter [6].

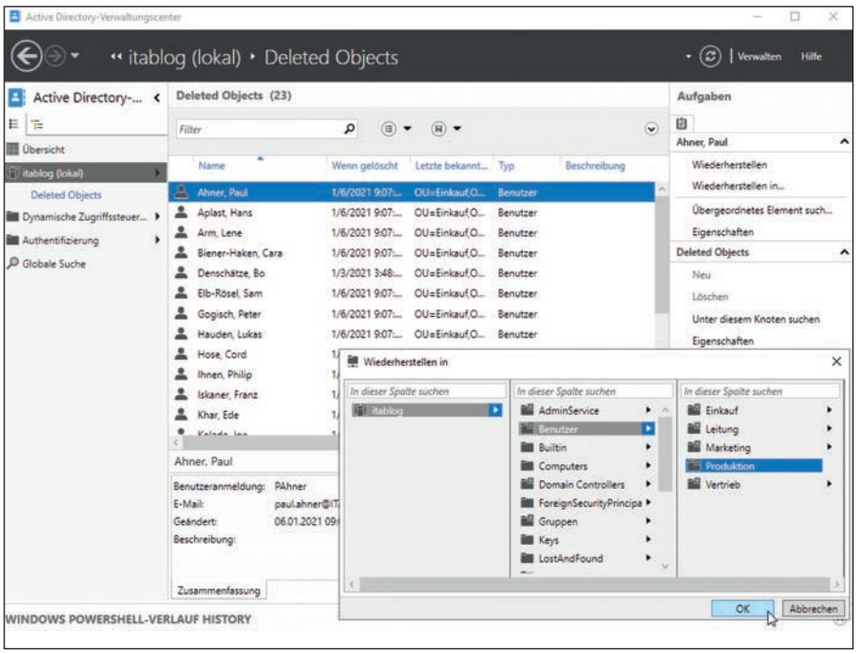

Bild 2: Der AD-Papierkorb holt gelöschte Objekte zurück, auf Wunsch auch in eine andere als ihre ursprüngliche OU.

Cmdlets einbinden, Snapshots erstellen

Im Archiv mit dem Skript finden Sie zusätzlich eine Datei mit zahlreichen Beispielen für die Verwendung der Cmdlets. Befindet sich das Skript etwa im Pfad "C:\Scripts\AD_Snapshot", binden Sie es mit den folgenden Kommandos in einer PowerShell-Sitzung ein und zeigen die verfügbaren Cmdlets an:

```
Set-Location C:\Scripts\AD_Snapshot

. .\AD_Snapshot_Functions.ps1

Set-Location C:\

dir Function: | Where-Object
  {$_.Name -like "*-ad*"}
```

Mittels des New-ADSnapshot-Cmdlets erzeugen Sie einen Snapshot mit dem aktuellen Stand der AD-Datenbank und zeigen per *Show-ADSnapshot* alle bereits vorhandenen Snapshots an. Der Befehl

```
Mount-ADDatabase -Last -LDAPPort 33389
```

mountet den jüngsten Snapshot. Auf aktuellen Systemen mit einer PowerShell in der Version 3 oder neuer zeigt

```
Mount-ADDatabase -Filter -LDAPPort 33389
```

alternativ einen grafischen Dialog an, aus dem Sie den gewünschten Snapshot auswählen (Bild 3). Das Cmdlet stellt den Snapshot als separaten LDAP-Server auf dem TCP-Port 33389 bereit. Dabei öffnet das Tool Dsamain ein separates Fenster, das Sie nicht schließen dürfen. Dsamain beendet sich selbsttätig und schließt das Fenster automatisch, sobald Sie nach getaner Arbeit den Snapshot mittels *Dismount-ADDatabase* wieder aushängen.

Attribute wiederherstellen

Solange der Snapshot eingebunden ist, können Sie Attribute im produktiven AD mit dem Versionsstand des alternativen LDAP-Servers vergleichen und mittels des Repair-ADAttribute-Cmdlets mit den Werten aus dem Snapshot überschreiben. Mit

```
Get-ADUser <SamAccountName> -Proper-
  ties Description,Department
  -Server localhost

Get-ADUser <SamAccountName> -Proper-
  ties Description,Department
  -Server localhost:33389
```

stellen Sie für einen bestimmten Benutzer die Werte der Attribute "Beschreibung" und "Abteilung" im laufenden AD und im Snapshot gegenüber. Haben Sie die Werte versehentlich geändert, überschreibt

```
Get-ADUser <SamAccountName> |
  Repair-ADAttribute -Property
  Description,Department -LDAPPort
  33389
```

die Attribute im Livesystem wieder mit den ursprünglichen Werten aus dem Snapshot. Das Kommando

```
Get-ADUser -Filter {name -like "A*"}
  | Repair-ADAttribute -Property
  Description,Department -LDAPPort
  33389 -WhatIf
```

leistet dasselbe für alle Benutzer, deren Name mit dem Buchstaben "A" beginnt. Der bei einer großen Anzahl an Zielobjekten sehr zu empfehlende Parameter "-WhatIf" sorgt in diesem Fall dafür, dass Ihre Anweisung zunächst nur ausgibt, was geschehen würde. Sind Sie mit dem Ergebnis zufrieden, führen Sie den Befehl noch einmal ohne diesen Parameter aus.

Einen Spezialfall stellt die Mitgliedschaft in Gruppen dar. Beim Attribut "MemberOf" eines jeden Benutzers handelt es sich um einen sogenannten Back-Link, da die Mitgliedschaft primär nicht am Benutzerkonto, sondern an der Gruppe hängt. Möchten Sie die Gruppenmitgliedschaften eines Benutzers aus dem Snapshot wiederherstellen, hilft dabei das separate Repair-ADUserGroup-Cmdlet. So fügt

```
Get-ADUser <SamAccountName> |
  Repair-ADUserGroup -LDAPPort 33389
```

einen Benutzer wieder allen Gruppen hinzu, in denen er sich zum Zeitpunkt des Snapshots befand.

Snapshots regelmäßig einplanen

Zusätzlich zu Systemstatus-Backup und AD-Papierkorb bieten Ihnen die AD-Snapshots somit eine einfache Möglichkeit, fehlerhaft manipulierte Objekte im AD zu reparieren. Es handelt sich dabei allerdings nicht um eine Wiederherstellung im eigentlichen Sinn, da die Cmdlets unerwünschte Schreibvorgänge nicht rückgängig machen, sondern neuerlich überschreiben.

Listing: Snapshot als geplante Aufgabe

```
Set-Location c:\scripts\AD_Snapshot
. .\AD_Snapshot_Functions.ps1
Set-Location c:\
New-ADSnapshot
Remove-ADSnapshot -Keep 5 -Last
```

Um für den Ernstfall gerüstet zu sein, sollten Sie das Erzeugen von Snapshots mittels New-ADSnapshot-Cmdlet auf einem oder besser mehreren DCs in Ihrer Umgebung als regelmäßige Aufgabe einrichten und dabei den verfügbaren Speicherplatz nicht außer Acht lassen. Dabei hilft Ihnen das zusätzliche Remove-ADSnapshot-Cmdlet, mit dem Sie ältere Snapshots aufräumen. So automatisiert ein minimales PowerSell-Skript zur lokalen Ausführung als geplante Aufgabe auf einem DC dieses Vorhaben und behält dabei nur die letzten fünf Versionen (siehe gleichnamiges Listing). Die mitgelieferten Beispiele der Cmdlets zeigen Ihnen alternativ, wie Sie die Kommandos per PowerShell-Remoting auch aus der Ferne auf einem oder mehreren DCs ausführen.

Sonderfall: Gruppenrichtlinien

Zu guter Letzt werfen wir noch einen Blick auf einen weiteren Spezialfall, die Gruppenrichtlinien. Zu jedem Gruppenrichtlinienobjekt (Group Policy Object, GPO) findet sich in der AD-Datenbank ein Objekt vom Typ "Group Policy Container" (GPC) mit seiner eindeutigen ID unterhalb des Zweigs "CN=Policies, CN=System, DC=itablog, DC=local". Mit den folgenden beiden Kommandos vergleichen Sie den Bestand an GPOs im laufenden System mit dem verbundenen Snapshot:

```
Get-ADObject -Filter 'objectClass
  -eq "groupPolicyContainer"'
  -Properties Name,displayName
  -SearchBase "CN=Policies, CN=Sys-
  tem, DC=itablog, DC=local" -Server
  localhost | ft Name,displayName

Get-ADObject -Filter 'objectClass
  -eq "groupPolicyContainer"'
  -Properties Name,displayName
  -SearchBase "CN=Policies, CN=System,
  DC=itablog, DC=local" -Server local-
  host:33389 | ft Name,displayName
```

Die Befehle liefern jeweils eine Tabelle mit den eindeutigen IDs und den Anzeigenamen zurück. Ist eines der GPOs abhandengekommen oder fehlerhaft, helfen Ihnen diese Informationen allein jedoch nicht weiter. Die eigentlichen Einstellungen des GPOs sind nicht Teil der AD-Datenbank, sondern liegen in Form von Ordnern und Dateien in der SYSVOL-Freigabe Ihrer Domäne, in unserem Beispiel unter "\\ itablog.local \ SYSVOL \ itablog.local \ Policies". Sie sind im AD-Snapshot folglich nicht enthalten.

GPO-Backup und -Restore per Skript

Alternativ zur Wiederherstellung aus dem Vollbackup eines DCs hat Windows Server weitere Hilfsmittel mit an Bord. Bis Windows Server 2012 R2 installierte das Feature "Gruppenrichtlinienverwaltung" einige nützliche Skripte im Ordner "C: \ Program Files (x86) \ Microsoft \ GPMC Sample Scripts", mit denen Sie einzelne oder alle GPOs sichern und auch wiederherstellen konnten. Aktuelle Ausgaben von Windows

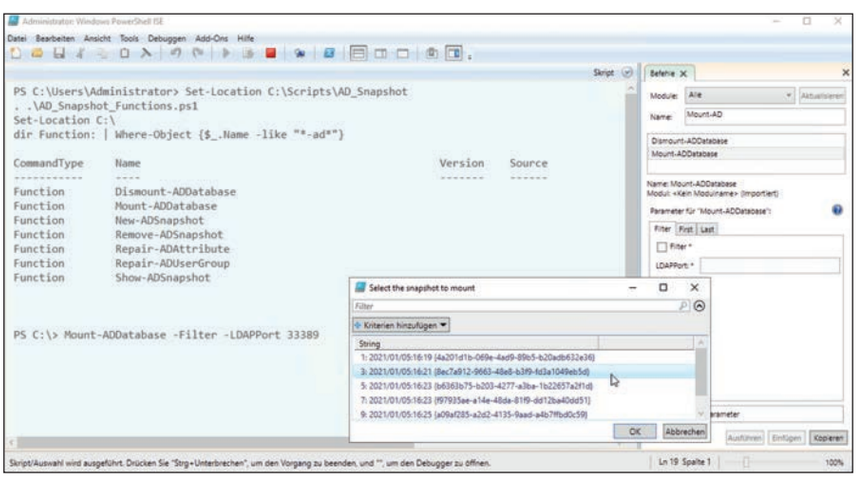

Bild 3: Per PowerShell-Cmdlet binden Sie Snapshots des ADs auf einem separaten LDAP-Port ein.

Server machen das Ganze noch einfacher, sie haben die passenden Werkzeuge in Form der PowerShell-Cmdlets "Backup-GPO" und "Restore-GPO" im Gepäck. Mittels

```
Get-GPO -All | Backup-GPO
  -Path <\\Zielserver\
  Freigabe\GPO-Backup>
```

schreiben Sie ein Backup aller GPOs in eine Netzwerkfreigabe. Ein lokaler Pfad funktioniert ebenso. Zu beachten ist dabei, dass der Befehl die GPOs im Zielpfad nicht unter ihrer eindeutigen ID abspeichert, sondern bei jeder Ausführung eine zusätzliche, für jeden Backupvorgang eindeutige Backup-ID vergibt. Der Vorteil besteht darin, dass Sie den Befehl wiederholt ausführen können, vorherige Sicherungen aber nicht überschreiben und somit mehrere frühere Versionsstände behalten. Der Nachteil ist, dass es abseits der grafischen Gruppenrichtlinienverwaltung schwierig wird, einzelne GPOs im Backup wiederzufinden. Erweitern Sie das Backup-Kommando daher, sodass es seine Rückgabe in eine Datei schreibt (Bild 4):

```
Get-GPO -All | Backup-GPO -Path
  <\\Zielserver\Freigabe\GPO-Backup>
  <\\Zielserver\Freigabe\GPO-
  Backup\Backup-IDs.txt>
```

Am besten richten Sie auch diesen Befehl als geplante Aufgabe auf einem DC ein. Mithilfe der Textdatei können Sie künftig einzelne Elemente der Sicherung einfach anhand von Anzeigenamen und eindeutigen IDs der GPOs, Backup-IDs sowie Zeitpunkt des Backups identifizieren. Mittels

```
Restore-GPO -All -Path <\\Zielser-
  ver\Freigabe\GPO-Backup>
```

setzen Sie alle GPOs wieder auf den Stand des letzten Backups zurück – ganz ohne die AD-Snapshots zu bemühen. Wahlweise eines der folgenden Kommandos

```
Restore-GPO -Name "<Anzeigename-des-
  GPOs>" -Path <\\Zielserver\Freiga-
  be\GPO-Backup>
```

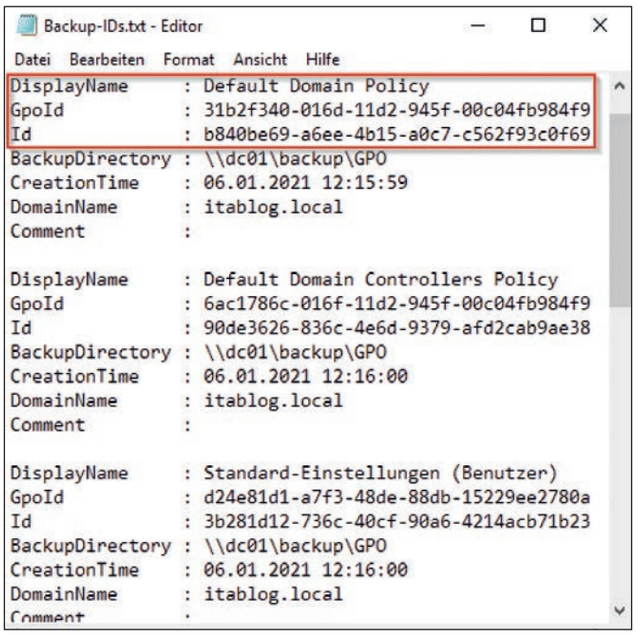

Bild 4: Backups einzelner GPOs identifizieren Sie anhand von Anzeigenamen, eindeutiger ID oder der Backup-ID.

beziehungsweise

```
Restore-GPO -GUID <Eindeutige-ID-
  des-GPOs> <\\Zielserver\Freigabe\
  GPO-Backup>
```

stellt den früheren Zustand eines bestimmten GPOs wieder her [7]. Allen zuvor genannten Aufrufen des Restore-GPO-Cmdlets ist aber eines gemein: Sie setzen ausschließlich die Einstellungen noch existierender GPOs auf den Stand der jüngsten Sicherung zurück. Haben Sie ein GPO nicht nur verändert, sondern versehentlich komplett gelöscht, bringt auch der Parameter "-All" es nicht wieder. Nicht mehr vorhandene GPOs können Sie nur anhand der zugehörigen Backup-ID reanimieren:

```
Restore-GPO -BackupID <Backup-ID-ei-
  nes-GPOs> <\\Zielserver\Freigabe\
  GPO-Backup>
```

Deutlich intuitiver gelingt die Wiederherstellung einzelner GPOs über die GUI der Gruppenrichtlinienverwaltung. Per Rechtsklick auf den Knoten "Gruppenrichtlinienverwaltung / Gesamtstruktur… / Domänen / <itablog.local> / Gruppenrichtlinienobjekte" erreichen Sie den Dialog "Sicherungen verwalten…". Greifen Sie hierüber auf das Sicherungsverzeichnis zu. Der Dialog zeigt Ihnen daraufhin alle im Zielpfad verfügbaren Backups einzelner GPOs übersichtlich an. Sie können dabei auch vollständig gelöschte Objekte wiederherstellen oder einfach nur deren Einstellungen anzeigen, um sie mit denen im Livesystem zu vergleichen.

Fazit

AD-Papierkorb, -Snapshots und die Sicherung von Gruppenrichtlinien sind praktische Ergänzungen zu einem Vollbackup. Alle vorgestellten Methoden und Tools sind kostenlos verfügbar und vereinfachen das Leben im Ernstfall ungemein. Machen Sie sich rechtzeitig mit den Werkzeugen und ihrer Handhabung vertraut, vorzugsweise zunächst in einer isolierten Testumgebung. Aktivieren Sie dann den AD-Papierkorb für Ihr produktives Active Directory und konfigurieren Sie auch geplante Aufgaben für regelmäßige Snapshots sowie GPO-Backups. Neben diesen technischen Aspekten dürfen auch eine Dokumentation Ihrer AD-Umgebung mitsamt Plan zur Wiederherstellung sowie regelmäßige Proben für den Ernstfall nicht fehlen. Der nächste Notfall kommt bestimmt. Gut vorbereitet können Sie diesem Ereignis ganz entspannt entgegensehen. *(jp)* IT

Link-Codes

[1] Wiederherstellung der AD-Gesamtstruktur
l4z11

[2] Tutorial: Authoritativer Restore von Active-Directory-Objekten
l4z12

[3] Active-Directory-Papierkorb
l4z13

[4] Aktivieren und Verwalten des Active-Directory-Papierkorbs im AD-Verwaltungscenter
l4z14

[5] Skript zum Wiederherstellen einzelner AD-Objekte
l4z15

[6] AD_Snapshot_Functions-PowerShell-Skript
l4z16

[7] Restore-GPO-Cmdelt erklärt
l4z18