Auszug aus...
IT DIRECTOR
Ausgabe 12/2010

Strategie für den Katastrophenfall

Das Active Directory ist von zentraler Bedeutung für eine Vielzahl von Systemfunktionen.

> Mitarbeiter brauchen Zugang zum Netzwerk, Zugriff auf Applikationen und Ressourcen und sind dabei auf ein störungsfreies Active Directory (AD) angewiesen. Applikationen von Exchange bis Sharepoint sind in ihrer Funktion ebenso davon abhängig. Die alltägliche Realität ist jedoch, dass Fehlfunktionen in Unternehmen aller Größen häufig auftreten. Menschliche Fehler sowie Hard- und Softwaredefizite führen leicht zu Beschädigungen des Active Directory, der Systemkonfiguration oder der Gruppenlinienobjekte. Jeder IT-Verantwortliche erlebt dies nur allzu oft.

Active-Directory-Objekte werden häufig geändert oder sogar entfernt: Der Admin löscht versehentlich Objekte, Mitarbeiter überschreiten ihre Zugriffsrechte, die angebundenen Applikationen haben unvorhergesehene Probleme und beeinträchtigen es. Die AD-Datenbank (NTDS.DIT) kann als Folge eines Hardware-Defekts beschädigt werden und fehlerhafte Scripte können AD-Attribute überschreiben.

Prinzipiell kann man unter drei Ausfallprinzipien unterscheiden: Das erste Szenario wäre der Ausfall eines oder mehrerer Domänencontroller (system failure). Dies verlangt ein DC Restore bzw. DC Deployment. Zweitens könnte es zum Verlust oder falscher Modifikation von Objekten (data corruption) kommen. Dann ist ein Online-Restore nötig. Das dritte Szenario kann ein Funktionsverlust der AD-Datenbank sein (database corruption). Dann hilft nur noch ein Domain/Forest Recovery.

Das Ergebnis dieser Probleme kann ein Systemausfall sein, in dessen Folge die Benutzerproduktivität stunden- oder gar tagelang verloren geht. Wie kann man möglichst schnell die gelöschten und geänderten Attribute und Objekte wiederherstellen? Der Markt bietet eine Reihe von Produkten, aber nur wenige tatsächliche Lösungen. Aus der langjährigen Erfahrung weiß der Anbeiter PC-Ware, dass gern auf den „Recovery Manager for Active Directory“ von Quest zurückgegriffen wird. Dieses Programm hat sich im Einsatz bei zahlreichen Großkonzernen bewährt. Quest hat damit als erster die Möglichkeit geschaffen, einzelne AD-Objekte – und später ganze DCs und AD-Strukturen – in kurzer

Zeit wiederherzustellen. Dies kann sogar dann ausgeführt werden, wenn auf dem Zielsystem eine andere Hardware als auf dem Quell-Server zum Einsatz kommt.

Gegenüber anderen Lösungen am Markt ist der „Recovery Manager for Active Directory“ nach wie vor am effektivsten. Wo die Wiederherstellung mit Konkurrenzprodukten Stunden dauern kann, benötigt er Minuten. Eine Schlüsselqualifikation für eine Recovery-Lösung, denn entscheidend ist eine rasch wieder hergestellte Produktivität. Mit der granularen Online-Wiederherstellung des Tools können im Remote-Zugriff ganze Bereiche des Verzeichnisses mit allen Inhalten und auch ausgewählte Objekte und Attribute wiederhergestellt werden, ohne dass man die Online-Verbindung des Active Directory unterbrechen muss. Da der Domänencontroller nicht neu gestartet werden muss, verkürzt sich die Wiederherstellungszeit erheblich.

Mit dem *entsprechenden Softwaretool lassen sich Systemausfälle in der Infrastruktur eines Unternehmens vermeiden.*

Dauerhafte Systemausfälle werden verhindert

Die meisten Recovery-Ansätze müssen manuell ausgeführt werden, sind zeitaufwendig und fehlerhaft. Mit „Recovery Manager for Active Directory“ haben sich diese Probleme minimiert. Es wird regelmäßig ein automatisches Backup des Active Directory erstellt, womit dauerhafte Systemausfälle verhindert werden können. Das Backup kann sowohl mit Agent als auch agentenlos ausgeführt werden. Damit sind sowohl User, Groups, Computer, GPOs und Konfigurationen als auch das Active Directory insgesamt wiederherstellbar. Mit der Reportingoption können Änderungsverfolgungen im Active Directory sogar aufgezeichnet und ausgewertet werden.

Für eine Recovery-Lösung sind noch andere Dinge von Relevanz: So unterstützt die Lösung auch Windows 2008 R2 und ermöglicht neben der Wiederherstellung von AD-Objekten auch komplette Rollbacks. Die Software fasst die automatischen Sicherheitskopien in ein verschlüsseltes Repository zentralisiert zusammen. Dies ist lokal, aber auch remote möglich. Über eine Management-Konsole kann die Wiederherstellung dann zentral gesteuert werden, wobei man online als auch offline vorgehen kann. Nach der Installation und der Einrichtung der Domänen wird immer das aktuellste AD-Schema zusammen mit einer Computer Collection und den zu sichernden Domänencontroller sowie ein erstes Backup geladen. Für jeden Active-Directory-Baum (Domänenname) gibt es einen separaten Container namens „Deleted Objects“, der alle gelöschten AD-Objekte aufführt und für einen Restore zur Verfügung stellt. In der Organisation dieses Containers liegt das – aus Sicht von PC-Ware – einzige Manko der Gesamtlösung, hier können die Quest-Entwickler noch nachbessern. Die gelöschten Objekte werden zwar alle vorgehalten, lassen sich jedoch erst nach aufwendigem Suchen finden. Hilfreich wäre eine Suchfunktion oder eine Sortierung der gelöschten Objekte, beispielsweise nach Benutzern. So wird in der aktuellen Version noch unnötig Zeit für die Forschung nach dem gelöschten Objekt aufgewandt. Im AD-Container „Domain Controllers“ gibt es die zusätzliche Option „Repair“. Hiermit kann ein Restore vom System State inklusive der AD-Datenbank und dem Sysvol eines Domänencontrollers gemacht werden. Der Repair Wizard bietet die Möglichkeit, individuell zu bestimmen, was wiederherstellt werden soll. Zur Auswahl stehen System State (vollständig), Active Directory (DIT und/oder Sysvol), Registry (SAM, Security, Software, System, Default, NTUser.dat), COM plus Class Registration Database, Boot Files und Performance Counters. Quest bietet ein Programm mit zahlreichen Recovery-Optionen und somit für fast jeden Fall die passende Lösung. Was diese Lösung zudem von anderen unterscheidet, sind die Möglichkeiten im Bereich „Online Restore von AD Objekten/Attributen“ und im Bereich „Recovery der Active Directory Datenbank“. Das automatische Backup und die Online-Wiederherstellungsmöglichkeit bieten optimale Unterstützung bei jeglichen Problemen, die bei der täglichen Arbeit mit Active Directory auftreten können. <

MICHAEL MEISTERS