ERNW
Enno Rey Netzwerke GmbH

ERNW Newsletter 6 / Januar 2005

Liebe Partner, liebe Kollegen,

willkommen zur sechsten Ausgabe des ERNW-Newsletters mit dem Thema:

Active Directory und Domänencontroller

Disaster Protection und –Recovery

von Friedwart Kuhn

fkuhn@ernw.de

Abstract:

Dedizierte Active Directory Disaster Protection- und dedizierte Active Directory Disaster Recovery-Strategien sind auch in größeren Active Directoy-basierten IT-Umgebungen noch keine Selbstverständlichkeit. Die hohe Integration von unternehmenskritischen Geschäftsprozessen in Active Directory macht aber genau dies erforderlich. Das vorliegende Dokument diskutiert ausgehend von einer Fallstudie Komplexität und Implikationen des Active Directory Disaster Recovery-Prozesses zusammen mit möglichen Vorsorgemethoden und gibt dabei einen Überblick über aktuelle Verfahren.

Inhalt

1. Einleitung

Nach wie vor sind viele große Unternehmen unzureichend vor einem Teil- oder Komplettausfall ihrer Server, bzw. ihrer Netzwerkinfrastruktur gerüstet. Dies ist – kurzgefaßt – das Ergebnis einer von Veritas-Software in Auftrag gegebenen Studie zum Thema Disaster Recovery in den Ländern Nord-Amerika, China, Asien, Europa und Benelux in Unternehmen mit mehr als 500 Mitarbeitern.[1] Die überwältigende Mehrzahl der IT-Verantwortlichen (95 Prozent) gibt dabei an, daß sie ohne einen Disaster-Recovery-Plan längeren bis langen Ausfallzeiten und materiellen sowie immateriellen Schaden zu entgegen zu sehen hätten. Als die beiden größten Bedrohungen wurden von den Befragten Soft- und Hardwarefehler (82 und 78 Prozent), gefolgt von Viren- und Hackerangriffen (69 Prozent), Krieg und Terrorismus (69 und 60 Prozent) angeführt.[2] Und obwohl 70 Prozent der Befragten mit Produktivitätseinbußen und jeweils 30 Prozent mit verschlechterten Kundenbeziehungen und mit Umsatz- und Gewinneinbußen rechnen, gibt es immer noch eine Reihe von Unternehmen in denen aufgrund von Mangel an finanziellen Mitteln, Mangel an technischem Know-How und vor allem durch Fehleinschätzung der eigenen Serversicherheit sowie der Folgeschäden eines größeren Ausfalls ein mit der heißen Nadel gestrickter und nur halbherzig implementierter Disaster Recovery-Plan existiert.

Das paradoxale Element einer solchen Situation liegt dabei in dem Mangel an Schutz durch Vorsorge gepaart mit der Komplexität aktueller IT-Systeme und der teilweise extrem hohen Abhängigkeit geschäfts- und zeitkritischer Anwendungen von eben diesen Systemen. Active Directory ist hier nur einer vor mehreren NOS-Verzeichnisdiensten, der aufgrund seiner hohen Integrationskraft in größeren Unternehmen eines besonderen Schutzes und einer *dedizierten Vorsorge* für den Katastrophenfall bedarf.

[1] Siehe: http://www.zdnet.de/itmanager/kommentare/0,39023450,39126634,00.htm .
[2] Siehe den in der vorausgehenden Anmerkung genannten Artikel.

Viele Unternehmen lösen die Frage der Vorsorge durch Support Service Level-Verträge mit externen Dienstleistern, in denen i. d. R. Reaktions- und Recovery-Ziele (wiederherzustellende Infrafstruktur, Recovery-Zeit) definiert werden, und manche Unternehmen machen die schmerzhafte Erfahrung eines Totalausfalls, ohne entsprechende Vorsorge getroffen zu haben. Sowohl Unternehmen, die Support Service-Verträge mit einem hochen Sicherheitslevel abgeschlossen haben, als auch jene, die keine oder wenig Vorsorge getroffen haben und im Notfall dann auf externe Dienstleister zurückgreifen müssen, machen eine gemeinsame schmerzhafte Erfahrung: Die Dienstleistungen sind für denjenigen, der den einen wie den anderen Dienst in Anspruch nimmt, meistens recht teuer (paradoxalerweise stellt die Firmenleitung einer unzureichend geschützten Infrastruktur *nach* Eintreten eines Katastrophenszenarios die seit Monaten oder Jahren von der IT geforderten Mittel meistens binnen Tagen oder Wochen bereit). Dabei muß eine gute Vorsorge nicht unbedingt teuer sein: flexible, effiziente *und* kostengünstige Active Directory- und Domänencontroller Disaster Protection, bzw. flexible, effiziente *und* kostengünstige Active Directory- und Domänencontroller Disaster Recovery ist möglich. Beides kann realisiert werden durch die Erweiterung starrer, einseitig-traditioneller Recovery-Lösungen (Serverimages /Datensicherungen auf Bandlaufwerken), und zwar durch eine Kombination aus spezifischem Active Directory Know-How und der Verwendung spezieller Softwaretools.

Vor der Implementierung irgend einer Lösung sollten jedoch zunächst die folgenden Erkenntnisse, die sich als Regeln formulieren lassen, stehen:

(1) Die Wiederherstellung von Active Directory und /oder Domänencontrollern mit Hilfe von Images ist i. d. R. problematisch und nicht empfehlenswert
(2) Active Directory Disaster Recovery ist ein komplexer Prozeß der ein tiefgreifendes und umfassendes Verständnis der Funktionsweise und Interaktion der verschiedenen Active Directory-Komponenten erfordert
(3) Effizientes Active Directory Disaster Recovery ist durch administratives Know-How und den Einsatz intelligenter Active Directory-Tools kostengünstig möglich

Wenn man (1) und (2) einmal akzeptiert (und verstanden) hat, dann besteht die Bereitschaft, über die Implementierung adäquater Lösungen für Active Directory Disaster Protection und – Recovery nachzudenken, und die Möglichkeit, auf eine sinnvolle Art und Weise eine für jedes Unternehmen individualisierte smarte, d. h. flexible, effiziente und kostengünstige Disaster Protection- und Disaster Recovery-Strategie zu entwickeln und zu implementieren. Ziel dieses Dokuments ist es, das IT-Management erstens für die Komplexität und die Implikationen des Active Directory Disaster Recovery-Prozesses zu sensibilisieren und zweitens auf die Möglichkeiten adäquate, effiziente und kostengünstige Lösungen bereitzustellen, aufmerksam zu machen.

2. Fallstudie

Die nachfolgende Studie soll helfen zu veranschaulichen:

- warum der Active Directory Disaster Recovery ein komplexer Prozeß ist, der eine profunde Kenntnis aller an Active Directory beteiligten Komponenten voraussetzt,
- weshalb eine Wiederherstellung von Domänencontrollern über klassische Imagingmethoden häufig keine gute Idee ist,
- daß schnelles Active Directory- und Domänencontroller-Recovery sowie der entsprechende vorbereitende Schutz *vor allem* durch Active Directory-spezifisches Know-How im Zusammenspiel mit der richtigen Methodik kosteneffizient möglich ist.

2.1 Szenario

Stellen Sie sich einmal das folgende Szenario vor: Ein größeres mittelständisches Unternehmen (ca. 1300 Angestellte, über 900 Desktops) betreibt eine Gesamtstruktur, die aus drei Domänen besteht. Die Desktoprechner, die einen Teil der holzverarbeitenden Maschinen steuern und weitere assoziierte Rechner sind in einer der Childdomänen integriert. Der erste von drei (Windows 2000, bzw. Server

2003-basierten) Domänencontrollern[3] dieser Childdomäne fällt aus. Die Verwendung einer speziell für die Firma geschriebenen Buchhaltungssoftware und die noch ausstehende Umstrukturierung des Active Directory-Entwurfs haben die Administratoren zum vorläufigen Beibehalten von zwei Windows NT 4.0-BDCs in der betroffenen Domäne erwogen.[4]

2.2 Vorgehensweise des Administrators

Einer der Administratoren des Unternehmens wird mit dem Festplattenausfall eines der drei Domänencontroller seiner Childdomäne konfrontiert. Der Ausfall, nehmen wir einmal an, fand am 5. Mai 2004 statt. Der Administrator verfügt über traditionelle Plattenimages, die er auf einem Bandlaufwerk gespeichert hat. Immerhin wird alle sechs Wochen ein solches Komplettimage von jedem Server angefertigt. Das letzte Image – vom 24. März – erweist sich als defekt, und kann daher nicht verwendet werden. Das vorletzte Image vom 11. Februar ist funktionstüchtig, doch nach dem Zurückspielen dieses Images kommt es zu einer Anhäufung von schweren Fehlern: Der Domänencontroller repliziert mit keinem weiteren Domänencontroller; sowohl domäneninterne[5] als auch domänenübergreifende Vertrauensstellungen funktionieren nicht mehr korrekt; viele Clients können sich nicht mehr an der Domäne anmelden, der Zugriff auf den SQL-Server, der auf einem NT 4.0-BDC läuft, funktioniert nicht mehr; das Systemprotokoll nicht nur des wiederhergestellten, sondern auch aller weiteren Domänencontroller wird mit diversen Fehlermeldungen angefüllt; - Benutzer der betroffenen Domäne können nicht mehr sinnvoll mit ihrem Desktop arbeiten, Benutzer der Gesamtstruktur können nur noch teilweise auf

[3] Für das Fallbeispiel ist es unerheblich, ob es sich um Windows 2000- oder Server 2003-basierte Domänencontroller handelt. Siehe auch die folgende Anmerkung.

[4] Der Einbezug von Windows NT 4.0-Domänencontrollern sowie die Funktionsebene(n) der Domäne(n), bzw. der Gesamtstruktur spielen hier eine vollkommen untergeordnete Rolle. Der Einbezug der Windows NT 4.0-Domänencontroller wirkt sich lediglich als weiterer in Betracht zu ziehender Faktor aus (und entsprach in dem hier diskutierten Fall der Wirklichkeit).

[5] Hier ist der sog. *Sichere Kanal* gemeint, über den während der Authentifizierung das lokal auf dem Mitgliedscomputer als LSA-Geheimnis gespeicherte Computerkennwort mit dem für diesen Computer im Active Directory gespeicherten Wert verglichen wird. Geraten beide – aus welchen Gründen auch immer – *out of sync*, dann kommt es zu einer Fehlermeldung, die das Fehlen einer Vertrauensstellung zwischen dem Computer und dem Domänencontroller, bzw. der Domäne bemängelt (vgl. dazu die KB-Artikel 216393, 325850 und 162797).

Ressourcen der betroffenen Domäne zugreifen. Der Administrator gerät in Panik und zwingt einen der nicht ausgefallenen Domänencontroller der betroffenen Domäne, die Rolle des PDC-Emulators zu übernehmen, um wenigstens eine funktionierende Anmeldung der Clients an der Domäne zu ermöglichen. Doch das verändert nichts an der Situation, viele Clients können sich nach wie vor nicht an der Domäne anmelden, Ressourcenzugriff ist nicht möglich, kurz: eine echte Katastrophe ist eingetreten. Es wird mit der Firmenleitung vereinbart, sofort externen Support zur Lösung des Problems in Anspruch zu nehmen.

Das dargestellte Szenario ist keineswegs fiktiv, es ist nur eines einer Reihe von ähnlichen Katastrophenszenarien, zu denen der Verfasser dieses Newsletters in mehr oder weniger regelmäßigen Abständen gerufen wird. Es sei dabei nur am Rande erwähnt, daß es auch nicht ungewöhnlich ist, mit einer oft *lückenhaften Dokumentation* über den physischen und logischen Aufbau der Gesamtstruktur, zu deren *A und O* FSMO-Rollenverteilung, Installationsdaten der Domänencontroller und die Aufbewahrung der Verzeichnisdienstinstallations-Protokolle auf den Domänencontrollern gehören, konfrontiert zu werden.

2.3 Fehler des Administrators

Was waren die Fehler des Administrators:

1. Vernachlässigung der *tombstoneLifetime*: Der *entscheidende* Fehler liegt in der Unkenntnis eines für das Verständnis der Funktionalität von Active Directory-Backups wesentlichen Faktoren: des Active Directory-Attributs *tombstoneLifetime*. Die *tombstoneLifetime* definiert – sehr allgemein gesprochen – die Gültigkeitsdauer für ein Active Directory-Backup.[6] Im Active Directory gelöschte Objekte werden nicht unmittelbar physisch aus der Datenbank entfernt: Nach dem Löschen eines Objekts werden die meisten seiner Attribute enfernt, und das Objekt wird als ein sog. *Tombstone* (dt. *Grabstein*) markiert. Das Objekt residiert damit weiterhin – allerdings

[6] Zur *tombstoneLifetime* siehe beispielsweise: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/a_tombstonelifetime.asp. Siehe auch KB-Artikel 216993 und weitere Fachliteratur.

unsichtbar für Benutzer und Administratoren[7] – in der Datenbank und wird erst nach Ablauf der *tombstoneLifetime* physisch aus der Active Directory-Datenbank entfernt. Die *tombstoneLifetime* beträgt standardmäßig 60 Tage und ihr Wert kann – wovon ich i. d. R. dringend abrate – auf Domänenebene verändert werden. Um das sicherheitskritische Wiedereinführen gelöschter Objekte (sog. *Lingering objects*) aus Backups, die älter als die *tombstoneLifetime* sind zu unterbinden, hat Microsoft mit einigen Post-SP2 Hotfixes, bzw. definitiv mit SP3 für Windows 2000 die *strict replication consistency*[8] für wiederhergestellte Objekte, deren Alter die *tombstoneLifetime* überschreitet, eingeführt.[9] Sie sorgt dafür, daß kein Domänencontroller mehr mit einem Domänencontroller repliziert, der aus einem Backup, das die *tombstoneLifetime* überschreitet, wiederhergestellt ist. Der KB-Artikel beschreibt weitere Implikationen dieses Verhaltens von Domänencontrollern (ab Windows 2000 mit SP3)[10] und wie und unter welchen Bedingungen dieses Verhalten manuell geändert werden kann.[11]

2. Mangelhafte Dokumentation durch die Administratoren des Unternehmens: Zwischen dem 11. Februar und dem 5. Mai, und zwar – sagen wir einmal – am 20. April war ein weiterer Domänencontroller zur betroffenen Domäne hinzugefügt worden. Dieser von dem Administrator bei der Wiederherstellung des ausgefallenen Domänencontrollers nicht berücksichtigte Umstand verschlechtert die Situation weiter: Es gibt nicht nur Domänencontroller, die nicht mehr miteinander replizieren und zwei PDC-Emulatoren, von denen jeder für sich beansprucht, der einzige in der Domäne zu sein (Inkonsistenz im *Configuration-NC*)[12], der wiederhergestellte Domänencontroller kennt

[7] Einige wenige Tools können Tombstones über ein GUI darzustellen; zu ihnen gehört der *Quest Recovery Mananger* (siehe auch weiter unten in diesem Whitepaper).
[8] Beachte: die Multimasterreplikation folgt innerhalb der *tombstoneLifetime* dem Prinzip der *losen Konsistenz*, d. h. Replikate verschiedener Namenskontexte (außer dem Schema-NC) müssen nicht konsistent sein (konvergieren allerdings gegen einen konsistenten Zustand).
[9] Vgl. KB-Artikel 317097. Auch wenn dies am Schluß des Artikels nicht erwähnt wird, gilt dieser ebenso für Server 2003.
[10] Also ebenso Server 2003-basierte Domänencontroller.
[11] Vgl. in diesem Zusammenhang auch die KB-Artikel: 314282
[12] Die schon in Windows 2000 implementierte Funktion des automatischen Sicherstellens der Singularität des PDC-Emulators setzt einen Abgleich der verschiedenen Replikate der

darüber hinaus den nach der Sicherung vom 11. Febrauar am 20. April hinzugefügten Domänencontroller noch nicht. Derartige Inkonsistenzen zwischen verschiedenen Replikaten kann die robuste Multimasterreplikation nicht von selbst auflösen: Die Replikationen zwischen dem wiederhergestellten Domänencontroller und seinen Replikationspartnern wird für die betreffenden Namenskontexte angehalten. Weitere Folgen der falschen Wiederherstellung machen eine auch nur ansatzweise geregelte Arbeit in der betroffenen Domäne unmöglich.[13]

3. Wiederholte Unkenntnis des Administrators: die Erzwungene Übernahme der PDC-Emulatorfunktion auf einen funktionierenden Domänencontroller hat zusammen mit der Wiederherstellung der Active Directory-Sicherung, die älter als die *tombstoneLifetime* ist, zu zwei PDC-Emulatoren für den gleichen Domänennamen mit den bekannten Folgen[14] geführt.

2.4 Ausweitung zu einem *Worst case*

Dieses Katastrophenszenario läßt sich in Gedanken fortsetzen und ohne viel Phantasie zu einem echten *Worst case* für das Unternehmens ausmalen:

- Stellen Sie sich vor, der wiederhergestellte Domänencontroller wäre Brückenkopfserver für einen Standort gewesen, dann wäre damit

---

Domänencontroller und damit eine Replikation zwischen diesen voraus. Genau diese ist aber wg. der *strikten Replikationskonsistenz*, bzw. wegen des Überschreitens der *tombstoneLifetime* bei der Wiederherstellung des ausgefallenen Domänencontrollers nicht möglich, so daß der Zustand der Inkonsistenz der Datenbanken zwischen dem wiederhergestellten Domänencontrollern und seinen potentiellen Replikationspartnern nicht automatisch aufgelöst werden kann.

[13] Solche Folgen sind: doppelte Netbios-Namen (für die betroffene Domäne) im Netzwerk mit allen Implikationen (Fehlermeldungen von WINS-Servern, vorübergehende Deaktivierung der doppelten Namen mit dem Zugriffsverlust auf die entsprechende Ressource); vollständige Störung des Betriebs von NT 4.0-BDCs, die zwei verschiedene PDCs für den gleichen Domänennamen nicht interpretieren können (daher der Zugriffsverlust auf den SQL-Server); Zugriffsverlust von Clients auf Ressourcen der Domäne (Computer- /Benutzerkonten, die dem wiederhergestellten Domänencontroller noch nicht bekannt sind, aber von diesem authentifiziert werden sollen; dito für in der Zwischenzeit abgelaufene Kennwörter; sog. Vertrauensstellungen zwischen Mitgliedsservern der Domäne und dem wiederhergestellten Domänencontroller, die abgelaufen sind und per Hand aktualisiert werden müssen) etc.

[14] Siehe vorausgehende Anmerkung.

dieser Standort für die betroffenen Namenskontexte vollständig von der eigenen Gesamtstruktur abgeschnitten.

- Stellen sie sich vor der falsch wiederhergestellte Domänencontroller wäre RID-Master gewesen und es wären neue Benutzer nach der Wiederherstellung auf diesem Domänencontroller angelegt worden, dann wären doppelte RIDs und damit identische SIDs mit allen Implikationen in der Domäne die wahrscheinliche Folge.
- Angenommen der wiederhergestellte Domänencontroller wäre der Schemamaster der Gesamtstruktur gewesen und angenommen zwischen dem Zeitpunkt der Wiederherstellung (5. Mai) und dem Zeitpunkt der Sicherung (11. Februar) hätte eine Schemaerweiterung stattgefunden, z. B. durch die Integration von Exchange in Active Directory, dann wäre wahrscheinlich die Gesamtstruktur als Ganzes wiederherzustellen...[15]

2.5 Alternative: eine mögliche, den Umständen entsprechende Lösung

Wie sieht eine vernüftige Lösung des Problems unter den gegebenen Voraussetzungen (Fehlen eines Disaster Recovery-Planes, mangelhafte Dokumentation) aus:

1. Der Administrator informiert sich mit Hilfe diverser Tools (adsiedit.msc, ntdsutil.exe, ldp.exe, replmon.exe, repadmin.exe, dcdiag.exe, netdiag.exe) über: FSMO-Rollenverteilung, Globale Katalog-Server-Verteilung, Brückenkopfserver, Replikationstopologie, Domänencontroller-Status und Replikationsstatus

[15] (!)...Weitere Implikationen, die aber keine prinzipiell neuen Erkenntnisse mit sich bringen, lassen sich denken: etwa die zwischenzeitliche Hinzufügung einer neuen Domäne; die Annahme der falsch wiederhergestellte Domänencontroller wäre ein Server 2003-basierte Domänencontroller und Host einer Anwendungspartition gewesen; ganz zu schweigen von zusätzlichen Serverfunktionen, die auf dem falsch wiederhergestellten Domänencontroller hätten ausgeführt werden können.

2. In Bezug auf die FSMO-Rollenverteilung muß abgewogen werden, welches der beiden folgenden Szenarien schwerer wiegt /drastischere Konsequenzen hat:
    a. Die Nicht-Verfügbarkeit der ausgefallenen FSMO-Rolle(n) für den Zeitraum, den eine Wiederherstellung des ausgefallenen Domänencontrollers benötigt
    b. Die Implikationen, die eine Funktionsübernahme der ausgefallenen Rolle(n) auf einen anderen Domänencontroller mit sich bringt[16]
3. Nach der Analyse werden ggf. die unverzichtbaren Rollen (i. d. R. nur der PDC-Emulator) übernommen.[17] In bezug auf die Übernahme sind allerdings bestimmte Implikationen für die evtl. spätere Wiederherstellung des ausgefallenen Domänencontrollers zu beachten:
    a. Ausgefallene Domänencontroller, von denen die Betriebsmasterrollen RID, Schema und Domänennamen übernommen wurden *dürfen nicht wieder online* gehen: Im Falle des RID-Masters ist die Sicherheit der Domäne in Frage gestellt ist, im Falle des Domänennamen- und besonders des Schemamasters die Integrität (und Funktionstüchtigkeit) der Gesamtstruktur.[18]

[16] Diese Entscheidung hängt maßgeblich von der auf dem Domänencontroller ausgeführten FSMO-Rolle(n) ab: Handelt es sich bei den ausgefallenen Rollen um die Betriebsmasterrollen für das Schema oder die Domänennamen, dann ist es i. d. R. zu verantworten, daß dieses Funktionen eine zeitlang nicht zur Verfügung stehen. Gleiches gilt für den Ausfall des Infrastrukturmasters. Ist jedoch die Funktion des RID-Masters betroffen, dann können keine neuen Sicherheitsprincipals in der Domäne erstellt werden. Eine ausgefallene PDC-Emulatorfunktion wird sich – abhängig von weiteren Faktoren – i. d. R. sofort bemerkbar machen und muß daher wahrscheinlich übernommen werden. Aber auch weitere Faktoren können eine Rolle spielen. So ist zu klären, für welche weiteren Dienste und Funktionen der ausgefallene Domänencontroller als Host fungierte (einziger Domänencontroller an seinem Standort? Globaler Katalog? DNS-Server? Host einer Anwendungsverzeichnispartition? Um nur die wichtigsten Beispiele zu nennen. Eine erschöpfende Diskussion der notwendigen Abwägung hängt von mehren Faktoren ab und kann hier nicht durchgeführt werden).

[17] Siehe vorausgehene Anmerkung.

[18] Dies ist eine Faustregel; Ausnahmen, die nur unter besonderen Bedingungen möglich sind und ein tiefgreifendes Verständnis der Active Directory-Interna erfordern, bestätigen die Regel. Es muß also beispielsweise bei der Übernamme der Rolle des Schemamasters berücksichtigt werden, daß der Domänencontroller, von dem diese Rolle übernommen wurde als solcher (mit evtl. weiteren Funktionen, die dieser Domänencontroller ausgeführt hat) *nicht wiederhergestellt werden darf*. Noch einmal: dieser Domänencontroller mit seiner IP-Adresse, seinem FQDN und den von ihm registrierten SRV-Ressourceneinträge darf nicht wiederhergestellt werden. Seine Metadaten sind manuell aus dem Active Directory zu entfernen. Dieses Beispiel verdeutlicht die Notwendigkeit einer Disaster

   b. Die Betriebsmasterrollen des PDC-Emulaters und der Infrastruktur können problemlos übernommen werden, und ausgefallene Domänencontroller, die eine oder beide Funktionen ausgeführt haben können – im Zeitrahmen der *tombstoneLifetime* – problemlos wiederhergestellt werden

4. Nacharbeiten werden erledigt: Ggf. werden neue Globale Kataloge und Brückkenkopfserver definiert, nicht mehr verwendbare Replikationsverbindungsobjekte gelöscht, neue erstellt, die DNS-Namensauflösungstopologie überprüft (war der Domänencontroller DNS-Server, war *Bedingte Weiterleitung* aktiviert?), der Domänencontroller- und Replikationsstatus sowie die Replikationstopologie überprüft. Die Behandlung der Metadaten des ausgefallenen Domänencontroller wird geklärt, ebenso die von diesem Domänencontroller stammenden SRV-Ressourceneinträge.

Für einen erfahrenen Active Directory-Administrator läßt sich die hier aufgeführte Vorgehensweise unter den gegebenen Umständen zusammenfassen zu:

1. Analyse der Situation (meint hier der Active Directory-Implikationen)
2. (Angenommen ein dritter Windows 2000- oder Server 2003-basierter Domänencontroller soll möglichst schnell wieder verfügbar sein:) Neuinstallation von Windows 2000 Server oder Server 2003 auf einem neuen Rechner
3. Heraufstufung des Rechners zum Domänencontroller in der betroffenen Domäne

---

Recovery-Protection, und eine Folge dieses Beispiels könnte sein: Die Schemarolle wird auf einen dedizierten Domänencontroller der Gesamtstruktur gelegt, und dieser Domänencontroller führ *keine* weitere Funktion aus (nicht einmal die eines Active Directory-integrierten DNS-Servers). Weitere Überlegungen könnten mit einfließen: Um die gesamtstrukturweit singulären FSMO-Rollen und die administrativen Gruppen *Organisations-Admins* und *Schema-Admins* zu schützen, könnte für sie eine leere Forest-Root-Domäne eingerichtet werden. Ökononmische Überlegungen könnten zu einem Zusammenlegen der Rollen von Schema- und Domänennamenmaster auf einen Domänencontroller führen.- Sie sehen, wie stark eine gute Disaster Protection- und Disaster Recovery-Strategie von einem sicheren und durchdachten Design der Gesamtstruktur abhängt. Siehe in diesem Zusammenhang auch den ERNW-Newsletter 5 (https://www.ernw.de/newsletter/newsletter5_de.pdf).

4. Garantierung der Verfügbarkeit der PDC-Emulatorenrolle durch Übernahme der Funktion auf den besten dafür geeigneten Domänencontroller (der drei Domänencontroller)
5. Ausführen von Nacharbeiten

Für die Durchführung der ersten vier Schritte und damit die Wiederherstellung einer Situation, in der eine geordnete Funktion sowohl der Domänencontroller als auch der Clients der betroffenen Domäne möglich ist, braucht ein Active Directory-Administrator mit halbwegs aktueller Hardware auch unter ungünstigen Bedingungen nicht länger als 90 Minuten.

Diese 90 Minuten müßen den ca. 15 Stunden gegenübergestellt werden, die benötigt wurden um: das Problem mit seinen Implikationen durch Rekonstruktion zu analysieren, die erst duch die falschen Maßnahmen des Firmenadministrators entstandenen Probleme zu beseitigen und einen dritten Domänencontroller zur Verfügung zu stellen. Es erübrigt sich hinzuzufügen, daß der Betrag für die 15 Stunden geleisteten Support gut 33% der Kosten für die Implementierung einer Hochverfügbarkeitslösung für die betreffende Domäne oder alternativ ungefähr den Kosten für eine mögliche Schulung der Firmenadministratoren enspricht.[19]

[19] Dieser Vergleich hat natürlich plakativen Charakter, denn mit entsprechend geschulten Administratoren und/ oder der Implementierung von Disaster Protection und – Recovery-Methoden, hätte das geschilderte Katastrophenszenario erstens niemals solche Dimension angenommen (es wäre bei einem Festplattenschaden geblieben) und zweitens wäre die Gesamtstruktur nicht nur vor diesem, sondern auch weiteren (zukünftigen) Fehlern und Ausfällen geschützt.

3. Disaster Protection und Disaster Recovery – Optimierte Methoden

Optimierte Disaster Recovery-Methoden beinhalten nicht nur den Einsatz von Know-How und spezieller Technologie bei der Wiederherstellung, sondern beginnen mit der Implementierung einer für das Unternehmen sinnvollen Disaster Protection-Strategie.
Die zu implementierende Strategie hängt dabei im wesentlichen von der Definition der folgenden drei Faktoren ab:

1. Gewünschter Verfügbarkeitsgrad der Domänencontroller /Domäne /Gesamtstruktur (das impliziert auch die Differenzierung der Schutzbereiche: Schutz vor Hardwareausfall, vor Softwareausfall und /oder beidem)
2. Active Directory-, bzw. Standort-Design und der diesem zugrunde liegenden Replikationstopologie
3. Den von dem Untermehmen für Disaster Protection und Disaster Recovery bereitgestellten finanziellen Betrag

Zusätzlich zu berücksichtigende Faktoren könnten sein: das Know-How der Firmenadministratoren, und die Forderung der IT-Leitung, eingetretenene Fehler aus Sicherheitsgründen (Vermeidung von Wiederholung, Aufdeckung von System- und Sicherheitslücken) unabhängig von der Produktionsumgebung analysieren zu können (was die Investition in zusätzliche Hardware und idealerweise in Active Directory-Troubelshooting- und Analyse-Tools notwendig macht).

Mögliche Active Directory- und Domänencontroller-Disaster Protection-Strategien können bei einem Null-Kosten-Budget mit einer geschedulten Systemstatus- und einer zusätzlichen Registry-Sicherung[20] beginnen, führen über das Erstellen von je

[20] Eine zusätzliche Registry-Sicherung etwa mit *Regback.exe* (kann z. B. über eine Batchdatei automatisiert werden) kann u. U. einer günstigen Lebensversicherung für einen Domänencontroller /Server (überhaupt für jeden Windows-Rechner ab Windows NT 4.0) gleichkommen. Die Kernidee des

einer Antwortdatei für die automatisierte Installation nicht nur des Betriebssystems, sondern auch des Verzeichnisdienstes für jeden auf diese Art wiederherzustellenden Domänencontroller bis hin zu ausgefeilten Hochverfügbarkeitslösungen, wie die Sicherung von Domänencontroller-Platten auf einer SAN mit Hilfe von Schattenkopien und der damit verbundenen Möglichkeit einer Just-in-time-Wiederherstellung. Die Auflistung der verschiedenen Recovery-Methoden und eine kurze Diskussion liefert der folgende Abschnitt.

Disaster Recovery soll das passende Gegenstück zur Disaster Protection darstellen, so daß beide Methoden zwei ineinander greifende Teile einer einzigen Schutzstrategie und Methodik darstellen. D. h., daß die in der Disaster Protection-Strategie geforderten Bedingungen zu der implementierten Recovery-Methode passen müssen: Wenn z. B. der Verfügbarkeitsgrad einer Domänene 363 Tage pro Jahr (keine Schaltjahre) sein soll und man insgesamt nicht mit mehr als 3 Ausfällen[21] pro Jahr rechnen muß, dann darf die Recovery-Zeit für die betreffende Domäne 16 Stunden nicht überschreiten.[22]
Bei der Implementierung der passenden Disaster Recovery-Strategie sind also die folgenden mit der Disaster Protection-Strategie korrelierten Faktoren geeignet gewichtet zu bewerten:

1. Voraussetzungen für die Anwendbarkeit der Recovery-Methode (die klassische Wiederherstellung eines ausgefallenen Domänencontrollers über dessen Systemstatus-Sicherung erfodert z. B. die Bootbarkeit des Systems)
2. Implikationen der gewählten Recovery-Methode (die Wiederherstellung von Domänencontroller über Schattenkopien impliziert z. B. die Einarbeitung und das Training des administrativen Personals)

Winternals Recovery Managers basiert auf genau dieser Annahme (zusammen mit der Tatsache, daß bei Serversystemen Betriebssystemausfälle im statistischen Mittel mehr als 30 mal häufiger auftreten als Hardwarefehler).

[21] Dieser Wert läßt sich auf der Grundlage der eingesetzten Hard- und Software mit Hilfe von Statistiken bestimmen.

[22] Von diesem Wert ist die max. Latenzzeit bis zum Bemerken des Ausfalls der Domäne und dem Beginn des Recovery abzuziehen. Ggf. ist der Wert mit einem 'Sicherheitspolster' hinsichtlich der wahrscheinlichen Ausfallshäufigkeit sowie weiteren Faktoren zu gewichten.

3. Zeitaufwand für die Implementierung der der Recovery-Methode entsprechenden Disaster Protection-Strategie
4. Zu verkraftende Downtime des ausgefallenen Domänencontrollers bei der gewälten Recovery-Methode
5. Kostenaufwand für die zu implementierende Recovery-Methode

Recovery-Methoden von Domänencontrollern
(Reihenfolge der Anordnung in etwa nach den Kosten der Methode):

(1) Wiederherstellung aus einer Systemstatus-Sicherung

(2) Wiederherstellung aus einer ASR[23]-Sicherung

(3) Neuinstallation mit Hilfe von Antwortdateien

(4) Softwarebasierte intelligente Wiederherstellung mit Tools wie Winternals Recovery Manager

(5) Wiederherstellung aus einem Tape-Backup (mit Software eines Drittanbieters)

(6) Wiederherstellung aus einem Disk-to-Disk-Backup (mit Software eines Drittanbieters)

(7) Schnelle Wiederherstellung mit Hilfe von Schattenkopien

Diskussion:

(1) Jede der aufgeführten Methoden besitzt Vor- und Nachteile. Die ausschließliche Sicherung von Domänencontrollern über den Systemstatus wie sie in den traditionellen Microsoft-Kursen gelehrt wird ist fraglos die kostengünstigste Lösung, sie ist aber auch die zeitaufwendigste Lösung, da sie vor der eigentlichen Herstellung des Domänencontrollers immer die Wiederherstellung der Betriebssystemumgebung erfordert.[24] Die Systemstatussicherung unter Windows 2000 kann sich noch nicht des erst in Windows XP und Server 2003 möglichen

[23] *ASR* steht für *Automated System Recovery* (Automatische Systemwiederherstellung) und ist eine Option von *Ntbackup.exe* unter Server 2003 (und auch Windows XP). ASR steht unter Windows 2000 nicht zur Verfügung.

[24] Siehe dazu etwa das Whitepaper von Microsoft *Windows 2000 Server Disaster Recovery Guidelines*, das zwar sinnvolle und richtige Richtlinien anführt, dessen Disaster Recovery-Prozeß in der Praxis jedoch langwierig und aufwendig (dafür aber nahezu kostenneutral) ist.

Snapshots auf Basis von Schattenkopien bedienen, so daß gerade geöffnete Dateien nicht gesichert werden können. Dies betrifft auch vom Betriebssystem verwendete Dateien.[25]

(2) Schneller und umfaßender ist in jedem Fall die Wiederherstellung aus einer ASR-Sicherung, die den Einbezug von System- und Bootpartition gestattet und sogar Flexibiltät gegenüber dem Austausch von Festplattencontrollern bietet.[26] Wird in dem Domänencontroller eine zusätzliche Festplatte für ASR-Sicherungen zur Verfügung gestellt, und werden mindestens zwei ASR-Sicherungen innerhalb der *tombstoneLifetime* durchgeführt, dann kann ein ausgefallener Domänencontroller bei der Verwendung von aktueller Hardware binnen 30 min. komplett wiederhergestellt werden. Die ASR-Sicherung muß dabei nicht einmal auf dem gleichen pyhsischen Rechner wiederhergestellt werden, einzige Voraussetzungen sind: die Zielfestplatte darf nicht kleiner aus die Quellplatte sein und der HAL des Quellrechners muß mit der Hardware (vor allem dem Chipsatz) des Zielrechners zusammenarbeiten.[27] Mit ASR ermöglicht Microsoft erstmals eine vergleichsweise schnelle und flexible Wiederherstellungsmöglichkeit von komplett ausgefallenen Rechnern nahezu ohne Zusatzkosten. Soll die Wiederherstellung eines Domänencontrollers über einer Systemstatussicherung oder über einer ASR-Sicherung auf einer anderen Hardware erfolgen, sind zusätzliche Maßnahmen zu ergreifen.[28]

(3) Eine weitere Recovery-Strategie kann das 'Wiederherstellen' von Domänencontrollern über die automatisierte Installation mit Antwortdateien sein. Wenn pro Domäne und pro Sicherungsintervall[29] ein gutes Backup der *Ntds.dit* zur

[25] Eine Tatsache die Microsoft nicht deutlich beim Namen nennt und die in Windows 2000 zu fehlerhaften Systemstatussicherungen führen kann. Eine Abhilfe bietet erst der Schattenkopiendienst in Windows XP und Server 2003 oder die Verwendung von moderner Backup-Software, deren Filtertreiber die Fähigkeit besitzen, Schreib- und Lesezugriffe zwischenzuspeichern und für die Snapschußdauer einzufrieren.

[26] Jedoch erst ab Server 2003. Die Wiederherstellung eines Domänencontrollers aus einer ASR-Sicherung ist keine triviale Angelegenheit. Sie erfordert in jedem Fall eine Sonderbehandlung des *Ntfrs*-Dienstes. Siehe dazu u. a. den KB-Artikel 836421.

[27] Selbst wenn die HALs von Quell- und Zielrechner nicht übereinstimmen, gibt es manuelle Eingriffsmöglichkeiten, von denen ich jedoch abrate. Als Mindestanforderung sollten die HALs von Quell- und Zielrechner übereinstimmen. Idealerweise stimmen Quell- und Zielrechner überein.

[28] Siehe dazu die KB-Artikel: 263532 und 237556.

[29] Das Sicherungsintervall kann pro Domäne und pro Domänencontroller definiert werden und hängt von verschiedenen Faktoren ab (Dynamik der Veränderungen im Domänen-NC, geforderte Aktualität

Verfügung steht, kann eine kostengünstige und relativ schnelle 'Wiederherstellung' eines Domänencontrollers über die automatisierte Installation mit vorbereiteten Antwortdateien erledigt werden. Da die Replikation einer großen *Ntds.dit* viel Netzwerkbandbreite in Anspruch nehmen kann, eignet sich ein solches Verfahren in Windows 2000-Umgebungen nicht für Standorte, die über eine geringe Bandbreite angebunden sind. Server 2003-basierte Domänencontroller können dagegen durch die sog. *Install from media*-Option[30] mit dem letzten aktuellen Systemstatus eines Domänencontrollers ihrer Domäne während des Heraufstufens 'gefüttert' werden, so daß sie nur die seit diesem Zeitpunkt vorgenommen Änderungen über die WAN-Leitung replizieren müssen. Der Vorteil dieser Lösung ist ihre Kostenneutralität[31] und die vollkommene Unanbhängigkeit von der Hardware des ausgefallenen Rechners, dafür gilt es andere Implikationen wie z. B. das schon, bzw. noch vorhandene Computerkonto des Domänencontrollers zu berücksichtigen. Sind die entsprechenden Antwortdateien erstellt und die zu berücksichtigenden Implikationen einbezogen, kann ein Domänencontroller auf diese Art und Weise ohne großen Aufwand durch Neuinstallation wiederhergestellt werden.[32]

(4) Klassische Wiederherstellungsmethoden über Tapebackups, mit denen i. d. R. zunächst einmal eine Betriebssystemumgebung hergestellt wird, auf deren Basis dann die Wiedereinspielung eines guten Backups von Betriebssystem und Verzeichnisdienst erfolgen, sind relativ starre und unflexible Möglichkeiten. Sie entsprechen einer zeitkonsummierenden Holzhammermethode, die heutigen flexiblen Wiederherstellungsanforderungen oft nicht gerecht werden kann. Immer dann, wenn die Problemlösung nur einen granularen Eingriff wie die Wiederherstellung bestimmter Betriebssystem-spezifischer Dateien, bestimmter Dienstekonfigurationen oder eine granulare Wiederherstellung von bestimmten

---

der Sicherungen für Recovery-Zwecke, Archivierungsmethode und -budget). Als Randbedingungen kann man die beiden folgenden Regeln setzten: mindestens zwei gute Systemstatussicherungen pro Domäne und Sicherungsintervall, minimales Sicherungsintervall: zweimal innerhalb der *tombstoneLifetime* – dies ist das absolute Muß. Gut ist es, eine Systemstatussicherung pro 24h zu erstellen.

[30] *Dcpromo.exe /adv*.

[31] Allerdings ist die zu verwendende Antwortdateie zunächst einmal für jeden Domänencontroller individuell zu erstellen.

[32] Eines der großen Finanzinstitute Deutschlands hat sich für diese Domänencontroller-Disaster Recovery-Strategie entschieden.

Active Directory-Objekten erfordert, dann stellen die bisher genannten Wiederherstellungsmethoden von der klassischen Systemstatussicherung, über ASR und Tapebackups aus folgenden Gründen keine effiziente Methode dar:

1. Die seit des verwendeten Backups gemachten Änderungen gehen verloren
2. Die Rücksicherung verschlingt Zeit

Die *Gartner Group* kommt in einer Voraussage zu Datenschutz zu dem Ergebnis, daß Disaster Protection- und Recovery-Methoden in den nächsten Jahren stark an Bedeutung gewinnen werden und daß die traditionelle Recovery-Methode über Tapebackups /Replikation nur noch eine unter weiteren und flexibleren Recovery-Methoden sein wird.[33] Da die meisten Ausfälle auf Betriebssystemausfälle und nicht auf Ausfälle der Serverhardware zurückgehen, gewinnt die intelligente granulare Wiederherstellung zunehmend an Bedeutung.[34] So eignet sich so z. B. der *Recovery Manager* von *Winternals*[35] hervorragend, um ausgehend von der gewünschten 'Wiederherstellungsfläche' sog. *Recovery Sets* zu definieren. Diese können nur das Betriebssystem, das Betriebssystem und installierte Programme oder beliebig definierte Programm- und Benutzerdaten umfasen. Die *Recovery Sets* können zentral gespeichert und – entsprechende Berechtigungen vorausgesetzt – verwaltet werden, und auch ein Remoteboot sowie weitere Funktionalitäten können von einer Station aus vorgenommen werden. Rollbacks, auch von ganzen Rechnergruppen werden dabei über wenige Mausklicks ermöglicht. Diese intelligente Recovery-Methode, die auch die Auflistung von Veränderungen zwischen zwei Recovery Sets, die zu verschiedenen Zeitpunkten erstellt wurden, ermöglicht, läßt Verzeichnisdienstdaten und auf Wunsch Benutzerdaten unangetastet und ist zeiteffizient. Sie überwindet damit die o. g. Beschränkungen von traditionellen Backups.

---

[33] So heißt es: *In 2006, recovery will be the focus for data-protection activities, with traditional tape backup being only one approach to providing recovery within a specified time commitment* in: Raymond Paquet and Carolyn DiCenzo: *Predicts 2004: Recovery Replaces Backup and Replication.* Das dreiseitige Dokument mit der Nummer *SPA-21-3174* kann von den Seiten der Gartner Group www.gartner.com heruntergeladen werden.

[34] Betriebssystemausfälle treten in Windowsumgebungen im Mittel knapp dreimal so häufig wie Virusinfektionen und mehr als 30 mal häufiger als Serverhardwareausfälle auf. Vgl. dazu eine Statistik von *Veritas Software* auf den Seiten zu *Backup Exec*.

[35] Die aktuelle Version ist 2.0, vgl. www.winternals.com .

Auf Active Directory-Ebene gibt es ein Tool, das entsprechende Arbeit auf ähnlich intelligente Weise verrichtet: der mittlerweise von *Quest Software* vertriebene und aktuell in der Version 7.1 vorliegende *Quest Recovery Manager for Active Directory*. Dieses Tool bietet Lösungen für zahlreiche mehr oder weniger bekannte Hürden beim Umgang mit Active Directory-Wiederherstellungen:

- Online Wiederherstellung von einzelnen gelöschten (d. h. 'getombstonten') Objekten über ein GUI
- Korrektes Handling von Objekten mit verlinkten Active Directory-Attributen
- Aufzeichnung /Vergleich von Veränderungen verschiedener Active Directory-Backups
- Zentralisierte Administration sämtlicher *Ntds.dit*-Sicherungen aller Domänencontrollers der Gesamtstruktur

Schon die Möglichkeit einer granularen Online-Wiederherstellung einzelner Active Directory-Objekte über ein GUI macht das Tool zu einem unschätzbaren Begleiter für die tägliche Arbeit eines Active Directory-Administrators. Jeder Administrator, der unter Zeidruck einmal ein gelöschtes Benutzerobjekt, an dessen *DN* er sich gerade noch ungefähr erinnert, aus einer älteren Systemstatussicherung herstellen mußte, weiß um den Aufwand dieser Prozedur: Der Domänencontroller ist im Wiederherstellungsmodus neuzustarten; über *ntdsutil.exe* ist das entsprechende Benutzerobjekt authorisierend wiederherzustellen; der Domänencontroller ist wieder normal neuzustarten. Das funktioniert natürlich nur dann, wenn der exakte *DN* zum gelöschten Objekt bekannt ist. Oft ist aber genau der nicht mehr bekannt, so daß einem nur die authorisierende Wiederherstellung der ganzen das Objekt enthaltenden OU oder das Neuerzeugen des gelöschten Objekts incl. aller Nacharbeiten (Benutzerprofilkonfiguration, Gruppenmitgliedschaften, Rechtevergabe) übrigbleibt. Beide Lösungen sind zeitintensiv und unbefriedigend.[36] Betrachtet man die von Microsoft mitgelieferten Tools und deren Fähigkeiten, so gibt

[36] Und es gilt abzuwägen, ob der Aufwand für die Nacharbeiten an dem das gelöschte Objekt enthaltenden Container den Verlust des gelöschten Objekts nicht sogar überwiegen.

es unter Windows 2000 es keine Möglichkeit, *Tombstones* wiederherzustellen.[37] Zwar bietet sich ab Server 2003 die Möglichkeit *Tombstones* online zu 'reanimieren', doch dieser Prozeß ist zeitaufwendig, unbequem und fehleranfällig und stellt nur die für das 'Überleben' des Objeks wichtigen Attribute, keinesfalls jedoch das vollständige Objekt (mit allen Attributen vor dem Löschvorgang) wieder her.[38] Verfügt man also über keine zusätzliche intelligente Software Recovery-Lösung, dann gestaltet sich schon die Wiederherstellung einzelner Objekte als sehr zeitaufwendig und erfordert in jedem Fall zusätzliche Nacharbeiten.[39]

(5) Die Wiederherstellung mit Drittherstellersoftware über Tapebackups ist die traditionelle und bis heute am häufigsten verwendete Recovery-Methode. Bekannte und weitverbreite Lösungen sind *Backup Exec* von *Veritas Software* (die aktuelle Version ist 9.1) und *Bright Store ARCserve Backup* (aktuelle Windowsversion ist 11.1). Aber es gibt auch jüngere und /oder unbekanntere Vertreter dieser Methode wie *Symantecs Powerquest V2i Protector 2.0 (Server Edition)* oder der *True Image Server 7.0* von *Acronis Software*.[40] Doch auch der sinnvolle Einsatz solcher Lösungen setzt eine genauere Kenntnis der Arbeitsweise dieser Programme voraus: Während etwa *Backup Exec* vor der eigentlichen Wiederherstellung die Herstellung einer Systemumgebung verlangt, gestattet etwa der *V2i Protector* das Brennen einer bootfähigen Sicherung direkt auf CD oder DVD. Eine zeitgemäß zügige Wiederherstellung bieten in dieser Sparte damit nur Hersteller, die das Erstellen bootfähiger (CD-/ DVD- /Tape-) Serversicherungen gestatten. Ein

[37] Gelöschte Objekte können unter Windows 2000 über *ldp.exe* nur 'eingesehen' werden. Siehe dazu auch:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ldap/ldap/ldap_server_show_deleted_oid.asp vgl. auch den KB-Artikel 258310.

[38] Die entsprechende Prozedur wird u. a. in dem Artikel von Robbie Allen mit der ID *41576* auf www.winnetmag.com beschrieben.

[39] Einmal abgesehen davon, daß viele Administratoren nicht über das Know-How verfügen bestimmte Active Directory-Objekte, deren Wiederherstellung eine tiefere Kenntnis der Active Directory-Interna erfordert, sauber wiederherzustellen (so werden bei der authorisierenden Wiederherstellung eines Benutzerobjekts nicht notwendigerweise auch dessen Gruppenmitglieschaften und damit verbundene Zugriffsberechtigungen wiederhergestellt. Dies hängt damit zusammen, daß auch unter Server 2003 die Versionsnummer einer Gruppe nicht geändert wird, wenn ein Benutzerobjekt aus dem *memberOf*-Attribut der Gruppe entfernt wird, solange nicht die Gesamtstrukturfunktionsebene *Windows Server 2003* ist. Diese Verhalten betrifft auch andere, wenn auch nicht so sicherheitssensitive Objekte wie Benutzer. Und selbst wenn die Gesamtstrukturfunktionsebene *Windows Server 2003* ist, kann die Gruppenmitgliedschaft eines Benutzers aus Domäne A in Domäne B nicht wiederhergestellt werden).

[40] Spezielle Informationen zu der angeführten Software entnimmt man den Herstellerseiten.

Domänencontroller ist – halbwegs aktuelle Hardware vorausgesetzt – damit in 15 min. komplett wiederhergestellt.

(6) Vom Prinzip her identisch, jedoch teuerer als Tapebackup-Lösungen arbeiten Wiederherstellungsverfahren mit Disk-to-Disk-Backups. Sicherungen können damit noch schneller (und somit auch häufiger) erstellt werden, so daß der Datenverlust durch Änderungen beim Zurückspielen eines Backups klein gehalten werden kann. Außerdem verläuft der reine Recovery-Prozeß recht schnell. Eine solche Lösung erfordert jedoch eine ungleich höhere Investition in Hardware (i. d. R. *SAN* oder *NAS*) und ein Netzwerklayout, das die erforderliche Bandbreite bereitstellt.

Grundsätzlich gilt es zu beachten, daß sowohl Tapebackup- als auch Disk-to-Disk-Lösungen nicht die Granularität der in (4) betrachteten intelligenteren Verfahren besitzen. Intelligente Verfahren (4) und klassisches Recovery (über Tapebackups und Disk-to-Disk-Backups) eignen sich daher für unterschiedliche Recovery-'Flächen' (man denke etwa an die Wiederherstellung eines Domänencontrollers gegenüber der Wiederherstellung einer Betriebssystemkonfiguration oder eines gelöschten Active Directory-Objekts).

(7) Die teuerste, aber dafür schnellste Lösung ist die *Schnelle Active Directory Wiederherstellung mit Hilfe des Schattenkopiendienstes (VSS) und des Virtuellen Festplattendienstes (VDS)*.[41] Das dahinter stehende Prinzip ist das Folgende: Zusätzliche zu den mindestens zwei Domänencontrollern pro Domäne[42] wird ein dedizierter Backup-Server verwendet, der mit einem traditionellen Tape verbunden ist und auf dem die (vom Hersteller der Storagelösung gelieferte) Software zur Verwaltung der Schattenkopien installiert ist.[43] Die Domänencontroller brauchen dabei über keine lokalen Festplatten zu verfügen, sondern sind über einen SAN-

[41] Für eine detaillierte Beschreibung, siehe das White Paper von Microsoft *Windows Server 2003 Active Directory Fast Recovery with Volume Shadow Copy Service and Virtual Disk Service* unter:

http://www.microsoft.com/windowsserver2003/technologies/activedirectory/W2K3ActDirFastRec.mspx . Diese Lösung bedient sich zweier Dienste, die erst mit Server 2003 zur Verfügung stehen (VSS und VDS) und ist damit nicht für Windows 2000 geeignet.

[42] Aus sicherheitstechnischer Perspektive erfordert diese Active Directory Disaster Protection-Lösung nicht mehr als zwei Domänencontroller; die größe und das Design der Domäne könnten jedoch weitere Domänencontroller erforderlich machen.

[43] Dies kann z. B. *CommVault Galaxy* (ab V. 7.0) sein; dazu gehört insbesondere der *CommVault Shadow Explorer*, der zusammen mit dem *Virtual Disk Service* von Server 2003 das transportieren /mounten von definierten Data Sets (z. B. von Schattenkopien) erlaubt.

Switch, der vom Hersteller der Storagelösung mit geliefert wird, mit der SAN verbunden. Die vom Hersteller der Storagelösung gelieferte Software ermöglicht im Zusammenspiel mit dem *Virtual Disk Service* von Server 2003[44] sowohl das Booten von SAN als auch das dafür notwendige Management der Schattenkopien (Lösen einer Schattenkopie vom Original; Sichern der Schattenkopie; virtueller Transport einer gesicherten Schattenkopie zum ausgefallenen Domänencontroller). Ist diese Lösung einmal installiert und der Schattenkopiendienst konfiguriert, dann ist jeder ausgefallene Domänencontroller – solange noch mindestens ein funktionierender Domänencontroller der betroffenen Domäne zur Verfügung steht – in weniger als 5 min. wiederhergestellt (inklusive der abgleichenden Replikation mit dem nicht ausgefallenen Parnter. Diese Lösung erfordert eine höhere Investition in das Storage Array und einen nicht sehr hohen Schulungsaufwand für das administrative Personal, ist im Gegenzug aber hocheffizient:

- Active Directory /Domänencontroller sind praktisch vollständig[45] sowohl vor Hardware- als auch vor Software-Ausfällen geschützt;
- Der Produktivbetrieb eines ausgefallenen Domänencontrollers kann nach ca. 5 min wieder aufgenommen werden, ohne daß sich das administrative Personal gleich um die Fehlerbeseitung /Fehleranalyse kümmern muß. Statt dessen kann die Ursachenklärung auf einen Zeitpunkt verschoben werden, an dem das administrative Personal über die dazu notwendige Zeit und Ruhe verfügt;
- Schattenkopien können vergleichsweise häufig erstellt werden (ihre Erstellung nimmt wenig Systemressourcen in Anspruch; Schattenkopien stehen aufgrund des SAN-Netzwerklayout praktisch instantan jedem Domänencontroller der Domäne zur Verfügung).

---

[44] Der ab Server 2003 zur Verfügung stehende *Virtual Disk Service* (*VDS*) stellt für Storagehersteller eine einheitliche Schnittstelle bereit, so daß für Server 2003 (wie auch die Administratoren) alle Storagesysteme gleich aussehen, deren Hersteller ihre Hardware mit VDS-Hardwaretreibern und ihre Software mit VDS-Writern versehen. Siehe auch:
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp?url=/Resources/Documentation/windowsserv/2003/all/techref/en-us/W2K3TR_vds_intro.asp .

[45] Den sehr unwahrscheinlichen Fall eines gleichzeitigen Ausfalls aller Domänencontroller ausgeschlossen.

Gleichwohl hängt auch die Implementierung dieser Lösung vom Active Directory-Design ab; so ist es z. B. nicht sinnvoll, die SAN Site-Grenzen überschreiten zu lassen.

In der Praxis empfiehlt sich in Abhängigkeit von den Disaster Protection- und Disaster Recovery-Zielen und den Kosten, die das Unternemen bereit ist dafür zu tragen, sowie in Abhängigkeit vom Active Directory-Design und der Größe des Unternehmens in der Regel eine Kombination verschiedener Methoden: Die Forest-Root-Domäne einer großen Organisation kann z. B. durch eine Hochverfügbarkeitslösung über Schatenkopien und eine NAS gesichert werden, ebenso lebenswichtige zeit- und geschäftskritische Domänen, von deren Funktionstüchtigkeit etwa Systeme von Finanzdienstleistern oder Produktionsanlagen abhängen. Weniger kritische Bereiche können mit klassischen Methoden gesichert werden, die zusammen mit intelligenten Tools wie dem *Recovery Manager for Active Directory* ausreichende Verfügbarkeit bei hoher Flexibilität bereit stellen. Unverzichtbar ist in jedem Fall ein gut geschultes und mit der Funktionsweise von Active Directory und den beteiligten Komponenten vertrautes administratives Personal, das sowohl die Implikationen einer authorisierenden Wiederherstellung oder einer FSMO-Rollenverlegung kennen muß (um nur zwei Kernaufgaben des Active Directory Recoverys zu nennen) als auch die ggf. aufwendige Fehleranalyse eines instabilen Active Directorys beherrschen soll.

4. Zusammenfassung

Effiziente, d. h. schnelle, sichere und kostengünstige Active Directory- und Domänencontroller Disaster Protection und –Recovery ist, bzw. sind möglich. Dabei stehen jedem Unternehmen eine Reihe von Lösungen zur Verfügung, die von der nahezu kostenneutralen Methode der Systemstatussicherung bis hin zur ausgefeilten Hochverfügbarkeitslösung mit SAN und dediziertem Backup-Server reichen. Ein sauberes Active Directory-Design, gut geschulte und mit der Active Directory-Implementierung ihres Unternehmens vertraute Administratoren erlauben

eine klare Definition der Active Directory Disaster Protection und –Recovery-Ziele und die sinnvolle, den Bedürfnissen des Unternehmens angemessene Implementierung einer Lösung. Die Fähigkeiten von Server 2003[46] gestatten dabei sowohl im Low Budget- als auch im technischen High End-Bereich Active Directory- und Domänencontroller-Sicherungs- und Wiederherstellungsmethoden, die sowohl flexible (und kostengünstige) Alternativen als auch Erweiterungen zu traditionellen Verfahren darstellen. Eine sinnvolle Kombination der dargestellten Lösungen zusammen mit fähigem administrativen Personal ist die beste Lebensversicherung für Ihre Active Directory-basierte IT-Umgebung.

Friedwart Kuhn

ERNW GmbH
Friedwart Kuhn
Active Directory-Teamleiter
Consultant & System Architekt

ERNW Enno Rey Netzwerke GmbH
Maaßstrasse 28
69123 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
Mobil +49 174 3278727
www.ernw.de

[46] In diesem Zusammenhang sind v. a. zu nennen: *ASR*, *VSS* und *VDS* sowie die Möglichkeit, 'getombstonte' wiederherzustellen.