Microsoft Certified Professional Systems Engineer

Thomas Joos

MCSE TRAINER

MCSE für Windows Server 2003

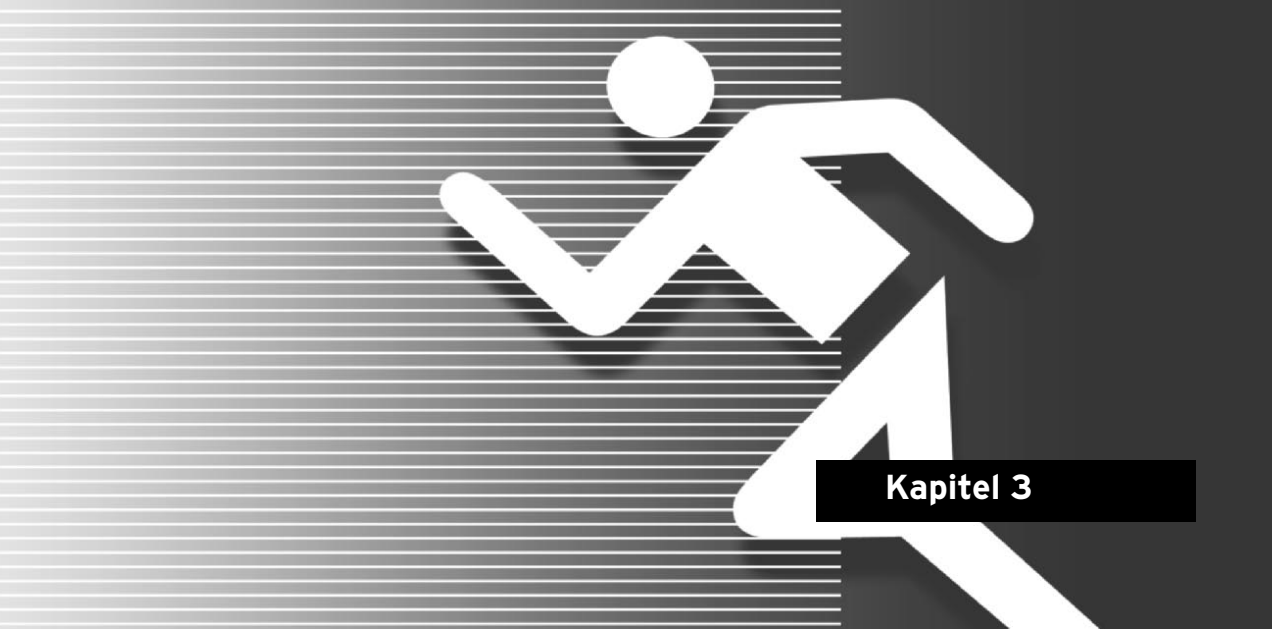
Die komplette Prüfungsvorbereitung inklusive Windows Vista

- **Für Examen 70-620, 70-270, 70-290, 70-291, 70-293, 70-294, 70-297 und 70-284**
- **Mit interaktiver, deutschsprachiger Prüfungssimulation auf CD**

180-Tage-Testversion von Windows Server 2003 auf zwei CDs

ADDISON-WESLEY

CD



Kapitel 3

Prüfung 70-290 – Verwalten und Warten einer Microsoft Windows Server 2003-Umgebung

Im Rahmen dieser Prüfung werden vor allem Themen im Bereich Benutzerverwaltung, Datensicherung, Verwaltung von Freigaben und dem IIS abgefragt. Für diese Prüfung benötigen Sie auch Informationen zum Software Update Service (SUS). Schauen Sie sich die Fragen aus diesem Kapitel und die Fragen zu 70-291 an und installieren Sie einen SUS in der Testumgebung. Der SUS hat keinerlei praktische Relevanz mehr, seit es den Nachfolger WSUS (Windows Server Update Services) gibt. Es reicht also durchaus, wenn Sie die Antworten der Fragen lernen und sich den SUS etwas anschauen. Vor den eigentlichen Prüfungsfragen gehe ich in diesem Kapitel wieder die Themen ausführlicher durch, die besonders häufig in den verschiedenen Formen in der Prüfung abgefragt werden. Neu in der Prüfung 70-290 sind die Simulationsaufgaben. Bei diesen Aufgaben müssen Sie spezielle Aufgabenstellungen während der Prüfung in einer Testumgebung durchführen. In diesem Kapitel zeige ich Ihnen, wie der optimale Ablauf bei der Bewältigung der einzelnen Simulationen ist. Sie sollten diese Simulationen ebenfalls in Ihrer Testumgebung durchführen. Auch wenn die Domänennamen und die Struktur der Aufgaben nicht immer genau zur Testumgebung passen, können Sie dennoch alle Aufgaben durchführen. Setzen Sie die Bedingungen der einzelnen Aufgaben dann einfach in Ihrer Umgebung und mit Ihrem Active Directory um. Lesen Sie sich auch die einführenden Abschnitte zur Prüfung 70-270 in Kapitel 2 durch. Viele Themen der Prüfung 70-270 werden auch in der Prüfung 70-290 behandelt.

Auch hier empfehlen wir Ihnen, parallel die Seite *http://www.mcse-certification.de* zu besuchen. Hier finden Sie weitere interessante Anleitungen zur Prüfung 70-291, die sich optimal mit diesem Buch ergänzen. Eine ebenfalls sehr interessante Informationsquelle für die Prüfungen 70-290 und 70-291 ist die Seite *http://support.microsoft.com/kb/917984/en*.

Fragen über die Erweiterung eines Servers und zur Überwachung von Leistungsindikatoren kommen quer durch alle Prüfungen immer mal wieder vor. Lesen Sie sich vor den Prüfungen die Informationen von dieser Seite durch:

`http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_mpmonperf_l3a.mspx?mfr=true`.

3.1 Gruppen in Windows Server 2003-Netzwerken

In der Prüfung 70-290 kommen bereits erste Fragen über die Gruppenkonzepte im Active Directory. In diesem Abschnitt gehe ich daher etwas näher auf die einzelnen Themen rund um die Benutzergruppen ein. Diese Themen haben nicht nur für die Prüfung Relevanz, sondern sind auch in der Verwaltung eines Active Directory von eminenter Bedeutung.

3.1.1 Gruppenarten im Active Directory

Im Active Directory werden die folgenden vier Typen von Gruppen unterschieden:

- Lokal
- Domänenlokal
- Global
- Universal

Lokale und domänenlokale Gruppen

Die lokalen Gruppen entsprechen dem Modell der lokalen Gruppen, das sich bisher schon bei Windows NT findet. In diesen Gruppen können Mitglieder aus allen Domänen der Gesamtstruktur, aus vertrauten Domänen, die in anderen Gesamtstrukturen definiert sind, und vertrauten Windows NT 4-Domänen enthalten sein. Hier können sowohl globale Gruppen und einzelne Benutzer und Computer aufgenommen werden. Unter dem Aspekt der Rechtevergabe haben sie nur Gültigkeit für das lokale System. Lokale Gruppen werden für die Zusammenfassung von globalen Gruppen oder in Ausnahmefällen von Benutzern eingesetzt, denen Zugriffsberechtigungen vergeben werden. Aus diesen lokalen Gruppen werden beim Schritt zum einheitlichen Modus von Active Directory automatisch domänenlokale Gruppen. Diese Gruppen können Mitglieder von überall enthalten, genauso wie lokale Gruppen. Der Unterschied besteht darin, dass diese Gruppen einheitlich auf allen Windows 2000-, Windows XP- und Windows Server 2003-Mitgliedssystemen und Windows NT-Maschinen der Domäne zu sehen sind. Sie verhalten sich damit letztlich so wie lokale Gruppen auf Windows NT-Domänencontrollern, die auf allen Domänencontrollern in der gleichen Weise verfügbar sind. Der Vorteil ist, dass damit eine lokale Gruppe im einheitlichen

Modus nur einmal pro Domäne definiert werden muss. Damit kann der administrative Aufwand zur sicheren Konfiguration von Clients signifikant reduziert werden.

Globale Gruppen
Die globalen Gruppen verhalten sich sowohl im gemischten als auch im einheitlichen Modus identisch mit den globalen Gruppen von Windows NT. Sie können Benutzer als Mitglieder enthalten. Diese Benutzer müssen zwingend aus der Domäne stammen, in der die globale Gruppe definiert ist. Globale Gruppen sind überall in der Gesamtstruktur sichtbar. Sie sind in vertrauten Gesamtstrukturen sowie in vertrauten Windows NT 4.0-Domänen verfügbar. Der wichtigste Unterschied ist, dass sie globale Gruppen der gleichen Domäne als Mitglieder enthalten können.

Universale Gruppen
Universale Gruppen können alle Arten von Gruppen und Objekten aus allen Domänen der Gesamtstruktur enthalten. Darüber hinaus können sie in allen Domänen einer Gesamtstruktur zur Rechtevergabe verwendet werden. Die universalen Gruppen vereinen daher die Vorteile der domänenlokalen Gruppen und der globalen Gruppen. Universale Gruppen sollten nicht exzessiv verwendet werden. Alle Informationen über Gruppenzugehörigkeiten zu universalen Gruppen werden auf den globalen Katalogservern gespeichert. Das bedeutet, dass jede Änderung repliziert werden muss. Wenn diese Gruppen in großer Zahl verwendet werden, kann das zu einem erheblichen Overhead bei der Replikation führen.

3.1.2 Verteiler und Sicherheitsgruppen

Der Gruppentyp kann bei der Erstellung und auch später aus zwei Optionen gewählt werden:

- *Sicherheit* definiert, dass es sich um eine Gruppe handelt, über die Zugriffsberechtigungen zugeordnet werden sollen. Diese Gruppen können auch parallel als Verteilergruppen verwendet werden, wenn ein Exchange-Server im Einsatz ist.
- *Verteiler* gibt an, dass die Gruppe nur für Verteiler in E-Mail-Programmen verwendet werden kann. Sie kann nicht für die Zuordnung von Zugriffsberechtigungen verwendet werden.

3.1.3 Verwenden von Gruppen für Berechtigungen

Die Vergabe von Zugriffsberechtigungen sollte immer an Gruppen erfolgen, da damit der geringste administrative Aufwand entsteht. Wenn ein weiterer Benutzer diese Berechtigung erhalten soll, muss er nur der Gruppe zugeordnet werden. Ebenso lassen sich die Zugriffsberechtigungen einzelnen Benutzern entziehen, indem diese einfach aus der Gruppe entfernt werden. Die Vergabe von differenzierten Zugriffsberechtigungen auf Dateien und Verzeichnisse ist nur bei Verwendung des NTFS als Dateisystem möglich. Auf Servern sollte generell mit NTFS gearbeitet werden. Bei der Planung von Berechtigungen sollten Sie sehr effizient planen, welche Ordnerstrukturen Sie anlegen und welche Gruppen Sie aufnehmen. Microsoft empfiehlt folgende Berechtigungsstruktur:

1. Domänenlokale Gruppe erhält Berechtigung auf Ordner und Freigabe.
2. Globale Gruppe(n) wird/werden in lokale Gruppe aufgenommen.
3. Benutzerkonten der Anwender sind Mitglieder in einzelnen globalen Gruppen.
4. Auf den Ordner im Dateisystem sollten die Administratoren *Vollzugriff* erhalten. Zusätzlich sollten Sie eine domänenlokale Gruppe anlegen, die Berechtigung auf Verzeichnisebene und auf Freigabeebene erhält. Domänenlokale Gruppen können alle anderen Arten von Gruppen aus dem ganzen Active Directory aufnehmen.
5. Die Anwender, die Zugriff auf diese Freigabe erhalten sollen, werden in eine globale Gruppe aufgenommen. Die globale Gruppe wird in die domänenlokale Gruppe aufgenommen, die Berechtigung auf den Ordner erhält.

Da die Anwender in globale Gruppen aufgenommen werden, können die Gruppen auch in andere domänenlokale Gruppen in anderen Domänen des Active Directorys aufgenommen werden. Das hat in großen Organisationen den Vorteil, dass Freigaben sehr effizient überall bereitgestellt werden können. Im Beispiel aus Abbildung 3.1 sehen Sie den Sinn dieses Konzepts:

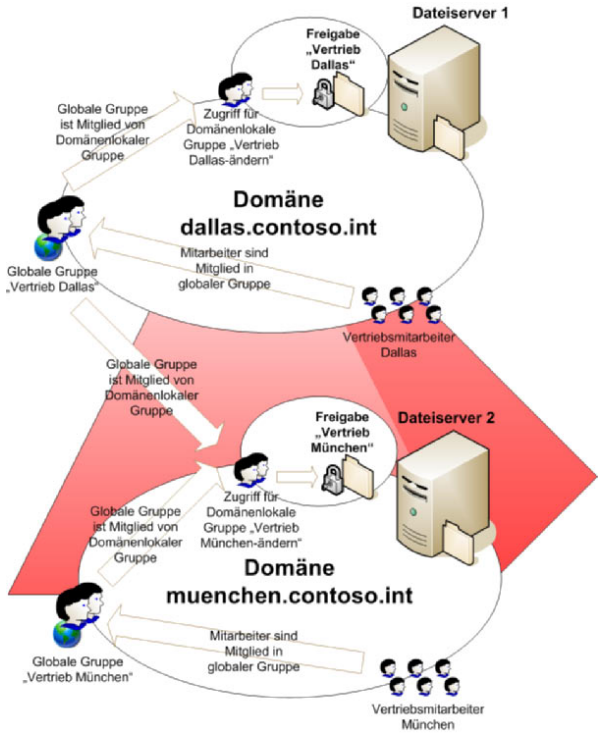


Abbildung 3.1: Beispielkonzept der effizienten Verwendung von Gruppen

- Domänenlokale Gruppen können globale Gruppen aus der kompletten Gesamtstruktur aufnehmen, können aber selbst nicht in anderen Domänen verwendet werden.
- Globale Gruppen können nur Mitglieder aus der eigenen Domäne aufnehmen, haben aber dafür die Möglichkeit, dass sie überall im Active Directory verwendet werden können.

Die Vertriebsmitarbeiter in Dallas können durch dieses Konzept sowohl auf die Freigabe in Dallas als auch auf die Freigabe in München zugreifen. Wenn neue Mitarbeiter Zugriff erhalten sollen, kann dies durch Aufnahme in die entsprechende globale Gruppe recht schnell erledigt werden. Zugriffsberechtigungen sollten nie ad hoc, sondern immer nur nach genau definierten Konzepten vergeben werden. Nur so lässt sich sicherstellen, dass mit einem durchdachten und damit sicheren Verfahren gearbeitet wird.

3.2 Betriebsmodi eines Active Directory

Ein Active Directory kann unter verschiedenen Betriebsmodi betrieben werden. Standardmäßig befindet sich das Active Directory nach der Installation im gemischten Modus. In diesem Modus können parallel zu den Windows Server 2003-Domänencontrollern auch noch Windows NT 4.0-Domänencontroller betrieben werden. Allerdings werden in diesem Fall nicht alle Funktionen und Möglichkeiten von Active Directory verwendet. Im Active Directory werden zwei verschiedene Ebenen der Betriebsmodi unterschieden:

- Betriebsmodus der einzelnen Domänen in der Gesamtstruktur
- Betriebsmodus der Gesamtstruktur

Während die Funktionsebene der Gesamtstruktur nur einmal verändert werden muss, müssen Sie für jede Domäne der Gesamtstruktur deren eigene Funktionsebene anpassen. Diese beiden Ebenen können jeweils unabhängig voneinander drei verschiedene Betriebsmodi annehmen:

- *Windows 2000 gemischt* – In diesem Modus können an der Domäne neben Windows 2000 und Windows Server 2003 auch Domänencontroller unter Windows NT 4.0 teilnehmen. Dieser Modus ist nach der Installation von Active Directory automatisch aktiviert.
- *Windows 2000 pur* – In diesem Modus können nur noch Windows 2000- und Windows Server 2003-Domänencontroller die Domäne verwalten. Es dürfen aber weiterhin Windows NT 4.0-Server als Mitglied betrieben werden. Ab diesem Modus können universelle Gruppen erstellt werden, und die SID-History wird unterstützt. Bei der SID-History können den Benutzerkonten mehrere SIDs aus anderen Domänen zugeordnet werden, zum Beispiel bei der Migration von Windows NT 4.0 zu Windows Server 2003 mit dem ADMT 3.0. Sicherheitsgruppen können in diesem Modus zu Verteilergruppen umfunktioniert werden.

- *Windows Server 2003* – Ab diesem Modus können Domänen in der Gesamtstruktur umbenannt und umstrukturiert werden. Es können gesamtstrukturübergreifende Vertrauensstellungen erstellt werden.

Sofern in einer Gesamtstruktur keine Windows 2000- oder Windows NT 4.0-Domänencontroller unterstützt werden müssen, sollten Sie so schnell wie möglich die Funktionsebene der Domänen und der Gesamtstruktur auf den Windows Server 2003-Modus hochsetzen. Sie erhalten dadurch keinerlei Nachteile, eröffnen sich aber erst dann die vollständigen Möglichkeiten von Active Directory.

Um die Funktionsebene einer Domäne hochzusetzen, klicken Sie im Snap-In Active Directory-Benutzer und -Computer mit der rechten Maustaste auf die Domäne und wählen die Option *Domänenfunktionsebene heraufstufen* (siehe Abbildung 3.2).

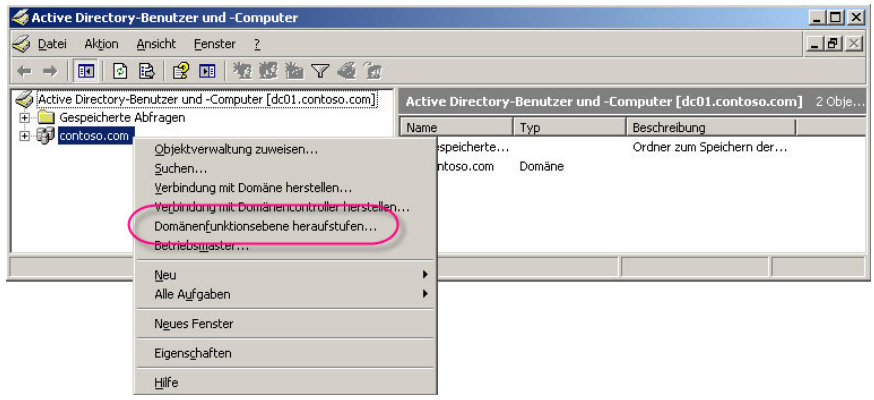


Abbildung 3.2: Heraufstufen der Domänenfunktionsebene

Sie erhalten eine Warnung, die Ihnen sagt, dass die Umstellung des Modus nicht mehr rückgängig gemacht werden kann. Wenn Sie diese Meldung bestätigen, wird die Funktionsebene heraufgestuft.

Die Funktionsebene der Gesamtstruktur können Sie mithilfe des Snap-Ins *Active Directory-Domänen und -Vertrauensstellungen* heraufstufen. Klicken Sie mit der rechten Maustaste auf das Menü *Active Directory-Domänen und -Vertrauensstellungen* und wählen Sie die Option *Gesamtstrukturfunktionsebene heraufstufen* (siehe Abbildung 3.3).

Hinweis

Sie können die Gesamtstrukturebene erst heraufstufen, wenn die Domänenfunktionsebenen aller Domänen der Gesamtstruktur heraufgestuft wurden.

Nach der Heraufstufung stehen die neuen Funktionen, wie SID-History, universale Gruppen und gesamtstrukturübergreifende Vertrauensstellungen, zur Verfügung.