

#### *Hinweis:*

Es wird davon ausgegangen, dass in der Quelldomäne Windows 2000 ausgeführt wird, und dass es sich bei der Zieldomäne um eine Windows 2003-Domäne im einheitlichen Modus von Windows 2000 oder höher handelt.

### **Einrichten von ADMT für eine Migration von Windows 2000 zu Windows Server 2003**

Sie können die Version 2 des Active Directory-Migrationsprogramms (ADMTv2) auf jedem beliebigen Computer installieren, auf dem Windows 2000 bzw. noch aktuellere Betriebssysteme ausgeführt werden.

Diese Betriebssysteme sind:

1. Microsoft Windows 2000 Professional
2. Microsoft Windows 2000 Server
3. Microsoft Windows XP Professional
4. Microsoft Windows Server 2003

Der Computer, auf dem Sie ADMTv2 installieren, muss entweder Mitglied der *Zieldomäne* oder der *Quelldomäne* sein.

### **Migration innerhalb einer Gesamtstruktur**

Bei einer Migration innerhalb derselben Gesamtstruktur ist es nicht erforderlich, spezielle Konfigurationseinstellungen vorzunehmen.

Das Konto, das Sie verwenden, um ADMT auszuführen, muss nur über ausreichende Berechtigungen verfügen, um die durch ADMT geforderten Aktionen durchführen zu dürfen.

So muss dieses Konto beispielsweise über die Berechtigung verfügen, Konten in der Quelldomäne zu löschen und Konten in der Zieldomäne einzurichten.

Bei einer Migration innerhalb derselben Gesamtstruktur werden die entsprechenden Daten und Dateien nicht kopiert sondern verschoben.

Diese Art der Migration wird zuweilen als destruktiv angesehen, da die migrierten Objekte nach dem Verschiebevorgang in der Quelldomäne nicht mehr vorhanden sind.

Da das Objekt verschoben und nicht kopiert wird, werden bestimmte Aktionen, die bei einer Migration innerhalb derselben Gesamtstruktur eigentlich optional sind, automatisch ausgeführt.

So werden *SIDHistory* (SID-Verlauf) und Kennwort bei allen Migrationen innerhalb derselben Gesamtstruktur automatisch migriert.

### **Migration zwischen verschiedenen Gesamtstrukturen**

In diesem Fall benötigt ADMT die folgenden Berechtigungen, um ohne Probleme ausgeführt werden zu können:

1. Administratorberechtigungen für die Quelldomäne
2. Administratorberechtigungen auf jedem zu migrierenden Computer.
3. Administratorberechtigungen auf jedem Computer mit zu konvertierender Sicherheit.

Bevor Sie eine Windows 2000-Domäne zu einer Windows Server 2003-Domäne migrieren, sind die nachstehend beschriebenen Domänen- und Sicherheitskonfigurationen vorzunehmen.

Bei einer Computermigration und einer Konvertierung der Sicherheit ist es nicht erforderlich, spezielle Konfigurationseinstellungen auf Domänenebene vorzunehmen.

Auf allen Computern, für die Sie eine Migration durchführen möchten, müssen jedoch die Freigaben **C\$** und **ADMIN\$** existieren.

Das Konto, das Sie verwenden, um ADMT auszuführen, muss über ausreichende Berechtigungen verfügen, um die durch ADMT geforderten Aktionen durchführen zu dürfen.

Das Konto muss in der Zieldomäne und in der Zielorganisationseinheit über die Berechtigung zum Einrichten von Computerkonten verfügen und außerdem auf allen zu migrierenden Computern Mitglied der lokalen Gruppe **Administratoren** sein.

### Migration von Benutzern und Gruppen

Legen Sie in der Konfiguration der Quelldomäne fest, dass der Zieldomäne vertraut werden soll. Optional kann die Zieldomäne darauf konfiguriert werden, der Quelldomäne zu vertrauen. Dies erleichtert zwar die Konfiguration, ist jedoch nicht erforderlich, um die ADMT-Migration abzuschließen.

### Anforderungen für optionale Migrationsaufgaben

Sie können die folgenden Aufgaben automatisch ausführen lassen, indem Sie den Assistenten für die Benutzermigration im Testmodus ausführen und die Option für die SIDHistory-Migration auswählen. Das Benutzerkonto, das Sie bei der Ausführung des ADMT verwenden, muss in Ziel- und Quelldomäne gleichermaßen über die Berechtigungen eines Administrators verfügen, damit die automatische Konfiguration erfolgreich sein kann.

1. Erstellen Sie in der Quelldomäne eine neue lokale Gruppe mit dem Namen **Quelldomäne\$\$\$**. Diese Gruppe darf keine Mitglieder enthalten.
2. Aktivieren Sie die Überwachung auf erfolgreiche bzw. fehlgeschlagene Überwachung der Kontenverwaltung in der Richtlinie für Standarddomänencontroller beider Domänen.
3. Konfigurieren Sie die Quelldomäne darauf, den RPC-Zugriff auf SAM zuzulassen, indem Sie den folgenden Registrierungswert auf dem PDC-Emulator in der Quelldomäne auf den **DWORD-Wert 1** festlegen:  
**HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\LSA\TcipClientSupport**

Sie müssen den PDC-Emulator neu starten, nachdem Sie diese Änderung vorgenommen haben.

*Hinweis:* Für Windows 2000-Domänen gilt, dass das für die Ausführung von ADMTv2 verwendete Konto in Ziel- und Quelldomäne gleichermaßen über die Berechtigungen eines Domänenadministrators verfügen muss. Für Windows Server 2003-Zieldomänen kann **Migrate SIDHistory** (SID-Verlauf migrieren) delegiert werden. Weitere Informationen dazu finden Sie in der Windows Server 2003-Hilfe.

Sie können die Kennwortmigration über Gesamtstrukturgrenzen hinweg aktivieren, indem Sie eine DLL installieren, die im LSA-Kontext ausgeführt wird. Durch das Ausführen in diesem geschützten Kontext können Kennwörter nicht unverschlüsselt eingesehen werden (auch nicht durch das Betriebssystem). Die Installation der DLL wird durch einen von ADMTv2 erstellten geheimen Schlüssel geschützt und muss durch einen Administrator durchgeführt werden.

Gehen Sie folgendermaßen vor, um die DLL für die Kennwortmigration zu installieren:

1. Melden Sie sich als Administrator oder mit einem Konto mit den Berechtigungen eines Administrators bei dem Computer an, auf dem ADMTv2 installiert ist.
2. Führen Sie über eine Eingabeaufforderung den Befehl ADMT-Schlüssel **QuelldomänePfad [\* | Kennwort]** aus, um die Kennwortexportschlüssel-Datei (.pes) zu erstellen. In diesem Beispiel steht Quelldomäne für den NetBIOS-Namen der Quelldomäne und Pfad für den Dateipfad zu dem Speicherort, an dem der Schlüssel erstellt wird. Es muss sich zwar um einen lokalen Pfad handeln, er kann jedoch auf ein Wechselspeichermedium verweisen, wie zum Beispiel ein Diskettenlaufwerk, ein ZIP-Laufwerk oder eine beschreibbare CD. Wenn Sie das optionale Kennwort am Ende des genannten Befehls eingeben, schützt ADMT die .pes-Datei mit diesem Kennwort. Wenn Sie das Sternchen (\*) eingeben, fordert ADMT die Eingabe eines Kennwortes, das bei der Eingabe nicht lesbar durch das System dargestellt wird.
3. Verschieben Sie die in Schritt 2 erstellte .pes-Datei auf den designierten Kennwortexportserver in der

Quelldomäne.

Dieser kann ein Domänencontroller sein, muss jedoch in jedem Fall über eine schnelle und zuverlässige Verbindung zu dem Computer verfügen, auf dem ADMT ausgeführt wird.

4. Installieren Sie die DLL für die Kennwortmigration auf dem Kennwortexportserver, indem Sie das Tool **Pwmig.exe** ausführen. **Pwmig.exe** befindet sich entweder im Ordner *1386\ADMT* auf dem Windows Server 2003-Installationsmedium oder in dem Ordner, in den Sie ADMTv2 aus dem Internet heruntergeladen haben.
5. Wenn Sie dazu aufgefordert werden, geben Sie bitte den Pfad zu der in Schritt 2 erstellten .pes-Datei ein. Dabei muss es sich um einen lokalen Pfad handeln.
6. Nach abgeschlossener Installation müssen Sie den Server neu starten.
7. Wenn Sie für die Migration der Kennwörter bereit sind, ändern Sie den folgenden Registrierungsschlüssel bitte so, dass er den **DWORD-Wert 1** aufweist.

Aus Sicherheitsgründen sollten Sie diesen Schritt erst dann ausführen, wenn die Vorbereitungen auf die Migration abgeschlossen sind.

**HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\LSA\AllowPasswordExport**

Sie können das ADMT von der folgenden Microsoft-Website herunterladen:

<http://www.microsoft.com/windows2000/downloads/tools/admt/default.asp>

Weitere Informationen zur Verwendung des ADMT für die Durchführung einer Migration finden Sie in der ADMT-Hilfe.