Übernahme einer NT4-Domäne mit Samba 3.0

Volker Lendecke
VL@Samba.ORG

3. April 2003

1 Einleitung

Seit Ende 2002 ist der offizielle Support von Microsoft für NT4 ausgelaufen oder zumindest deutlich eingeschränkt worden. Damit stellt sich für viele Unternehmen die Frage, wohin die existierenden Domänen migriert werden können. Der von Microsoft vorgeschlagene Weg ist ein Upgrade auf Windows 2000.

Ein Umstieg auf Windows 2000 bedeutet jedoch häufig auch gleich einen Wechsel auf die Domänenverwaltung mittels Active Directory. Dieser Verzeichnisdienst von Microsoft bringt eine Komplexität, die nur in wenigen Fällen wirklich benötigt wird.

Mit der Version 2.2 ist Samba in der Lage, die Anmeldung von Windows-Workstations als Primary Domain Controller zu übernehmen. Damit stellt sich die Frage, ob man wirklich Windows 2000 benötigt, um die existierende Domäne von einer weiterhin unterstützten Plattform kontrollieren zu lassen.

Mit der aktuellen Samba-Version 2.2 ist die Migration nur eingeschränkt zu empfehlen. Einerseits hat Samba 2.2 noch deutliche Einschränkungen als PDC, andererseits ist es noch nicht möglich, eine existierende Domäne direkt zu übernehmen. Das heißt, mit einer Migration müssen sämtliche Workstations und alle Benutzerprofile angefaßt werden, da Samba eine neue Domäne erstellt.

2 Benutzerverwaltung

Um die Probleme mit der Übernahme von NT-Domänen zu verstehen, muß erst einmal geklärt werden, was eine NT-Domäne und was ein Benutzer unter NT überhaupt ist.

Windows NT ist das erste Betriebssystem von Microsoft gewesen, das Konzepte wie Multitasking, Speicherschutz und Zugriffsrechte integriert hat. Zugriffsrechte bedeuten immer, dass es jemanden geben muß, dem Rechte gegeben werden können.

Unter Unix sind dies Benutzer und Gruppen. Hier beschränkt sich die Vergabe von Zugriffsrechten weitgehend auf die Rechtemasken auf Dateien. Anhand der Rechtemasken können Benutzern und Gruppen Zugriffsrechte vergeben werden. Dabei bestehen sowohl Benutzer als auch Gruppen in Unix nur aus einer kleinen Zahl. So etwas wie Benutzernamen kennt der eigentliche Unix-Kern überhaupt nicht. Dass man unter Unix selbstverständlich mit Benutzernamen arbeiten kann, ist eine reine Freundlichkeit der Anwenderprogramme wie `login` und beispielsweise `ls`.

In der PC-Welt hat es Anfangs das Konzept von Zugriffsrechten überhaupt nicht gegeben. Solange mit DOS, Windows 3 oder Windows 9x gearbeitet wurde, konnte sich jeder an einen PC setzen und loslegen. Es gab keinen Zugriffsschutz auf lokale Dateien und Verzeichnisse, jeder Benutzer konn-

te alles. Mit Windows NT ging dies nicht mehr, es kommt bei diesem System zwingend der richtigen Betriebssystemen bekannte Login-Prompt in einer graphischen Variante. Das heißt, um mit dem System arbeiten zu können, muß man zunächst Benutzer anlegen.

Um eine verteilte Benutzerverwaltung zu ermöglichen, gibt es unter Unix zur Zeit zwei Möglichkeiten: NIS und LDAP. NIS ist eine Entwicklung von SUN Microsystems, mit der im wesentlichen die Dateien `/etc/passwd` und `/etc/group` im Netz verteilt werden. Das heißt, jeder Unix-Rechner hat seine eigene lokale Benutzerdatenbank, die zufällig mit anderen Rechnern im Netz gleich ist. Auch unter LDAP ist das nicht anders: Alle Rechner haben ihre eigene Benutzerdatenbank, die sie von einer zentralen Stelle beziehen. Konzeptionell tun aber weder NIS noch LDAP viel mehr, als man mit einem echten Kopiervorgang nicht genau so gut erreichen könnte.

Warum betone ich so, dass jeder Unix-Rechner seine eigene Benutzerdatenbank hat? Unter Windows ist dies genau so, nur gibt es dort im Gegensatz zu Unix die Möglichkeit, dass jeder Rechner im Netz mehr als eine Benutzerdatenbank lokal zur Verfügung hat.

Das Unix-System der Benutzerverwaltung skaliert nicht besonders gut. Der Zahlenraum für User-IDs ist flach. Selbst wenn man mit 32-Bit User-IDs arbeiten kann und für alle möglichen Benutzer individuelle User-IDs vergeben kann, gibt es insbesondere dann Probleme, wenn Organisationen zusammengeführt werden müssen. Sich überschneidende User-IDs darf es nicht geben, es muss aufwendig umnummeriert werden.

3 Benutzer unter Windows NT, 2000 und XP

Was ist ein Benutzer unter Windows NT und folgenden? Jeder Benutzer wird durch einen sogenannten Security Identifier (SID) repräsentiert. Ein Security Identifier ist zweigeteilt: Der erste Teil ist 96 Bit lang und repräsentiert die Benutzerdatenbank, in der der Benutzer angelegt wurde. Der zweite Teil ist 32 Bit lang, heisst Relative Identifier (RID) und ist mit der Unix User-ID vergleichbar. Mit dem RID werden auf einem NT-System die einzelnen Benutzer unterschieden. Damit ist eine Benutzer-ID unter Windows NT 128 Bit lang, von denen 96 Bit bei der Installation eines Rechners so zufällig wie möglich gewählt werden. So bestehen gute Chancen, dass es einen Security Identifier nicht zweimal gibt.

Da an jedem SID die zugehörige Benutzerdatenbank sichtbar ist, kann man sehr einfach in einem NT-System mehr als eine Benutzerdatenbank gleichzeitig verwenden.

Nicht nur Benutzer, sondern alle Objekte, die Rechte erhalten können, werden unter NT durch Security Identifier repräsentiert. Das gilt insbesondere auch für Gruppen und Computer, die Mitglieder einer Domäne sind. Gegenüber Unix ergibt sich hier jedoch ein wesentlicher Unterschied: Der Zahlenraum der Relative Identifier wird von Benutzern und Gruppen gemeinsam genutzt. Unter Unix ist es möglich, daß es einen Benutzer mit der ID 1000 und gleichzeitig eine Gruppe mit der ID 1000 gibt. Beide haben nichts miteinander zu tun. Unter NT kann dies nicht passieren, ein Security Identifier ist grundsätzlich entweder ein Benutzer oder eine Gruppe. Dieser Unterschied ist der wesentliche Grund für die Schwierigkeiten, die Samba 2.2 mit der transparenten Übernahme einer NT4-Domäne hat, wie noch erklärt wird.

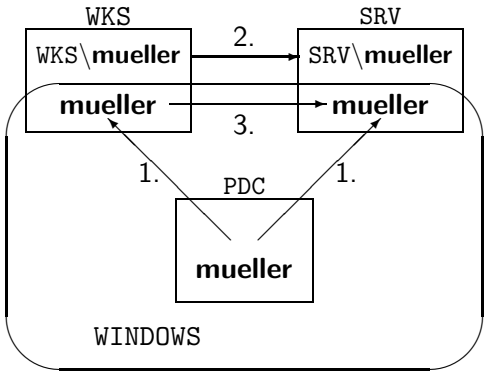
4 Windows NT-Domänen

Um die Administration von Workstations unter Windows NT erst zu ermöglichen, hat Microsoft das Domänenmodell entworfen. Eine theoretische Möglichkeit wäre, jeden Benutzer auf jedem beteiligten Rechner anzulegen. Aber selbst wenn man dieses sogenannte Peer-To-Peer-Modell sehr weitgehend automatisiert, skaliert es überhaupt

nicht. Die Alternative ist das Domänenmodell von Microsoft.

Mit dem beschriebenen Format der Security-Identifier ist es möglich, daß ein Rechner im Netz seine Benutzerdatenbank für den Online-Zugriff zur Verfügung stellt. Andere Rechner können diese Benutzerdatenbank so nutzen als sei es ihre eigene. Der exportierende Rechner heißt Domänencontroller, den alle Mitglieder der Domäne online zu allen Fragen rund um die Benutzerdatenbank kontaktieren.

Sobald eine Workstation Mitglied einer Domäne ist, kann ein Benutzer für seine Anmeldung aus mindestens zwei Benutzerdatenbanken auswählen. Der entsprechende Auswahldialog wird beim Anmelden präsentiert. Natürlich muß es den Benutzer auch in der entsprechenden Datenbank geben, damit er sich anmelden kann. Die folgende Abbildung soll die entsprechenden Verhältnisse verdeutlichen:



Den Benutzer **mueller** gibt es in dieser Abbildung dreifach: Auf der Workstation `WKS`, dem Server `SRV` und der Domäne `WINDOWS`. Den Benutzer **mueller** der Domäne `WINDOWS` läßt sich auf allen beteiligten Rechnern benutzen, die beiden anderen nur auf den jeweiligen Heimatrechnern des Benutzers.

Die unterschiedlichen Pfeile bedeuten im einzelnen:

1. Diese Verbindungen werden durch die Mitgliedschaft der Rechner in der Domäne erstellt. Die Mitglieder befragen den Domänencontroller nach allen Benutzerdaten.

2. Wenn keine Windows-Domäne eingesetzt wird, versucht Windows ein sogenanntes transparentes Login, sobald ein Server kontaktiert wird. Die Workstation speichert das vom Benutzer eingegebene Passwort und verwendet dies, sobald ein Server kontaktiert wird. Das transparente Login scheitert in dem Moment, in dem auf einem der beteiligten Rechner das Passwort des Benutzers geändert wird.

3. Diese Anmeldung wird als Netzwerk-Login bezeichnet. Auch hier benutzt die Workstation das gespeicherte Benutzerpasswort. Passwortänderungen sind in diesem Fall jedoch kein Problem, da der Server `SRV` die Gültigkeit des gelieferten Passworts online beim Domänencontroller nachfragt.

Jeder der drei Benutzer hat seinen eigenen SID, mit dem er von den anderen Benutzern unterschieden wird. Die Benutzernamen sind ebenfalls unterschiedlich: `WINDOWS`**mueller**, `WKS`**mueller** und `SRV`**mueller**.

5 Samba 2.2 und RIDs

Ist eine Maschine Mitglied einer Domäne, erfolgt die Zuweisung der Security Identifier zum Benutzer- und Gruppennamen durch den Domänencontroller. Samba als Domänencontroller muß genau wie NT für alle Benutzer und Gruppen Security Identifier generieren. NT selbst zählt beim Anlegen eines Benutzers einfach den höchsten verwendeten Relative Identifier um eins hoch und weist den daraus entstehenden Security Identifier dem Benutzer zu.

Samba generiert den Relative Identifier nicht anhand einer Tabelle, sondern errechnet diesen aus der Unix-ID des Benutzers oder der Gruppe. Dabei muss Samba das

oben beschriebene Problem der Überschneidung des Zahlenraums der Benutzer- und Gruppen-IDs berücksichtigen. Es gibt bei Unix-Systemen mit 32-Bit-IDs insgesamt 2^{33} Objekte, aus denen potentiell RIDs errechnet werden müssen. Samba geht davon aus, dass von dem Zahlenraum für Unix-IDs nur die untere Hälfte tatsächlich verwendet wird und errechnet RIDs anhand folgender Formeln:

$$\text{Benutzer-RID} = \text{Unix-UID} * 2 + 1000$$
$$\text{Gruppen-RID} = \text{Unix-GID} * 2 + 1001$$

Benutzer bekommen also gerade RIDs, Gruppen werden auf ungerade RIDs abgebildet. Mit diesen beiden Formeln ist es für Samba möglich, beide Richtungen zwischen NT-Welt und Unix-Welt ohne Tabelle zu berechnen.

6 Übernahme einer NT-Domäne

Wenn eine NT-Domäne durch einen anderen PDC übernommen werden soll, muß die gesamte Benutzerdatenbank übertragen werden. Dazu gehören insbesondere die Passwörter und die Security Identifier für alle Benutzer und Gruppen.

Ein erster Ansatz zur Übertragung der einer Domäne ist der Einsatz des Programms `pwdump2`. Dieses Programm können Sie auf einem Domänencontroller der existierenden Domäne aufrufen. Es liefert Ihnen eine Liste aller Benutzer der Domäne, inklusive RID und Passwort.

Wenn es möglich ist, die Workstations erneut in die Domäne aufzunehmen, können Sie mit diesen Informationen einen neuen Domänencontroller unter Samba 2.2 aufsetzen, der zumindest die Benutzerpasswörter erhält. Sie legen sämtliche Benutzer im Unix an und nehmen die Workstations ganz normal in die Domäne auf. Dann ergänzen Sie die `smbpasswd` um die fehlenden Benutzereinträge, die Sie von `pwdump2` erhalten haben. Dabei müssen Sie darauf achten, die Relative Identifier in der Ausgabe von `pwdump2` durch die Unix-UID zu ersetzen. Samba 2.2 setzt voraus, dass diese Werte gleich sind.

Beim nächsten Anmelden bekommt der Benutzer an der Workstation ein neues Profil, da sich die SID geändert hat. Um die Profile zu erhalten, müssen Sie die lokal gespeicherten Profile der Benutzer über die Systemsteuerung auf einen Server kopieren und dabei die Erlaubnis, das Profil zu benutzen, an „Jeder“ übergeben. In der neuen Domäne können Sie dann durch die Benutzung von servergespeicherten Profilen erreichen, dass der Benutzer sein altes Profil erhält.

7 Erhaltung von RIDs

Samba 2.2 ist bei der Verwendung der Datei `smbpasswd` nicht in der Lage, für jeden Benutzer einen Relative Identifier explizit abzuspeichern. Das liegt zum Teil daran, dass das Format der `smbpasswd` keinen Platz für einen RID hat. Wenn Sie Samba zusammen mit LDAP anwenden, dann werden Sie feststellen, dass es in der Objektklasse sambaAccount ein spezielles Attribut `rid` gibt. Das legt zumindest die Vermutung nahe, es könnte sich um einen Speicherplatz für einen individuellen Benutzer-RID handeln. Diese Vermutung ist absolut richtig.

Sie könnten also auf die Idee kommen, das LDAP-Verzeichnis manuell mit den aus `pwdump2` gewonnenen Daten zu füllen. Leider wird dieser Versuch nicht von Erfolg gekrönt sein, da Samba 2.2 an sehr vielen Stellen noch die oben beschriebene algorithmische Umsetzung von Unix-IDs in Relative Identifier voraussetzt.

Erst Samba 3.0 wird in der Lage sein, sich an das zu halten, was das LDAP vorschreibt.

8 Domänenübernahme Schritt für Schritt

Wenn Sie Samba 3.0 erfolgreich kompiliert haben, sind es nur wenige Schritte zur Übernahme einer Domäne von einem NT4-Domänencontroller. Samba wird für diese Übernahme quasi als Backup Domain Controller frisch installiert. Quasi deshalb, weil die Analogie mit einem echten NT-BDC nur bis zum Ende der Installation reicht, und nicht darüber hinaus.

Wenn Samba die Benutzerdatenbank vom PDC abzieht, muss die lokale Unix-Benutzerdatenbank mit den richtigen Benutzern automatisch versorgt werden. Genauso müssen die Gruppen korrekt angelegt werden. Dazu müssen die Parameter `add user script`, `add group script` und so weiter korrekt belegt sein.

Der zweite Schritt besteht darin, den Security Identifier des PDC in das lokale Samba zu übertragen. Dazu gibt es den Befehl `net rpc getsid`, der automatisch nach einem Domänencontroller sucht, und diesen nach seinem SID befragt. Schlägt dies fehl, haben Sie vermutlich ein Problem mit Ihrer NetBIOS-Namensauflösung.

Als nächstes müssen Sie die Domäne betreten, und zwar in der Rolle als BDC. Samba sieht sich selbst als BDC an, wenn Sie die folgenden beiden Parameter setzen: `domain master = no` und `domain logons = yes`. Sie müssen zusätzlich noch den Parameter `workgroup` auf den Namen Ihrer Domäne setzen. Danach können Sie mit dem Befehl `net rpc join -U Administrator` die Domäne betreten. An dieser Stelle ist wirklich die Angabe eines Domänenadministrators zusammen mit seinem Passwort notwendig, da im nächsten Schritt die komplette Benutzerdatenbank mit allen Passwörtern im Netz übertragen wird. Das Recht, Rechner in die Domäne aufzunehmen reicht hierfür nicht.

Wenn Sie die Domäne als BDC korrekt betreten haben und die entsprechenden Parameter aus dem ersten Schritt richtig gesetzt haben, dann bezieht der Befehl `net rpc vampire` die Benutzerdatenbank genau wie ein frisch installierender Backup Domain Controller vom PDC. Gleichzeitig legt Samba automatisch die korrekten Benutzer und Gruppen in der Unix-Benutzerdatenbank an und setzt RID und die anderen NT-Attribute korrekt.

Ist dieser Befehl erfolgreich durchgelaufen, können Sie den alten PDC abschalten und Ihren neuen PDC mit den Einstellungen `domain master = yes` und `domain logons = yes` zum PDC hochstufen.

Die existieren RIDs werden so an die Clients weitergegeben, wie sie der alte PDC gewählt hat. Neue Benutzer und Gruppen müssen von Samba weiterhin nach dem algorithmischen Schema ihre RIDs zugewiesen bekommen. Um nicht mit den vorhandenen RIDs in Konflikt zu kommen, müssen Sie als letzten Schritt noch den Parameter `algorithmic rid base` auf einen Wert setzen, der über allen von NT vergebenen RIDs liegt.