Künstler Burgy Zapp

Vereinfachte Prüfung von Zugangsberechtigungen mit IBM’s neuem EIM Feature in Verbindung mit Kerberos

von Patrick Botz

Server-Schnittstellen für Kerberos

Mit V5R2 hat IBM diverse Betriebssystem- und Client-Schnittstellen erweitert, um eine optionale Authentifizierung durch Kerberos zu ermöglichen. Die Schnittstellen wurden angepasst für: den iSeries Navigator, die PC 5250 Emulation, den Client-Teil des in OS/400 zur Verfügung gestellten ODBC-Treibers sowie für die Host Server, den NetServer, QFileSvr400, ODBC, JDBC, die Server innerhalb der DRDA-Architektur (Distributed Relational Database Architecture) und letztlich den Telnet Server auf der Host-Seite.

Der PC5250 Emulator (z.B. der Telnet Emulator, der mit iSeries Access for Windows ausgeliefert wird) lässt sich für die Kerberos Authentifizierung konfigurieren. Das hat zur Folge, dass ein Benutzer beispielsweise nach dem Start der Emulation ohne gesonderte Anmeldung direkt sein Anfangsmenü angezeigt bekommt oder dass sofort sein Startprogramm ausgeführt wird. Das wird möglich, da der Telnet Server auf EIM Informationen zugreift und der Benutzer bereits bei der Anmeldung an seinem System mit dem entsprechenden Benutzerprofil über Kerberos authentifiziert wurde.

Innerhalb des iSeries Navigators können sich Benutzer durch einfachen Mausklick auf einem System anmelden. Sie werden unter ihrem jeweils korrekten Benutzerprofil angemeldet, unabhängig davon, unter welcher Benutzer-ID sie in Windows 2000 angemeldet sind.

Die NetServer Erweiterungen bieten dem Benutzer die Möglichkeit, sich einen in OS/400 freigegebenen Ordner als Laufwerk zuzuordnen, ohne sich dem NetServer gegenüber erneut authentifizieren zu müssen. Aber hierbei besteht eine entscheidende Einschränkung: Der NetServer implementiert das Microsoft Software Message Block (SMB) Protokoll. Dieses Protokoll bedingt, dass wenn auch nur ein einziger PC Zugriff auf den NetServer nimmt, der nicht Windows 2000 oder eine spätere Version installiert hat, eine Authentifizierung über Kerberos nicht mehr zugelassen wird. Auch alle anderen PCs müssen sich dann über User-ID und Passwort gegenüber dem

NetServer neu authentifizieren.

QFileSvr400 kann man sich als das OS/400 Äquivalent zum NFS (Network File System) vorstellen. Es erlaubt Benutzern, dem lokalen OS/400 Dateisysteme zuzuordnen, die sich physisch auf einem fernen OS/400 befinden. Auch QFileSvr400 unterstützt nun Kerberos für die Authentifizierung.

Die Erweiterungen in ODBC, JDBC und DRDA SSO ermöglichen Benutzern nun die Ausführung von SQL oder selbst entwickelten ODBC (oder JDBC) Programmen über den iSeries Navigator. Das Interessante daran ist, dass das SQL Programm keine Prompts oder hart codierte User-IDs oder Passworte mehr enthalten muss. Das macht es nun möglich, Anwendungen wirklich multitiered (z.B. PC-zu-iSeries, iSeries-zu-zSeries, iSeries-zu-iSeries) und heterogen (z.B. Windows 2000, OS/400, zOS) zu entwickeln, wobei der einzige zu entwickelnde Code der Windows 2000 Code ist, der eine SQL Anforderung an ein iSeries System übermittelt. Der gesamte Rest bezüglich der notwendigen Authentifizierung wird von den Betriebssystemen mit Hilfe von EIM und Kerberos erledigt.

Durch die SSO- und EIM-Fähigkeiten ergeben sich in einer ganzen Reihe von Szenarien nützliche Auswirkungen. Stellen wir uns beispielshalber ein Unternehmen vor, das einen Benutzer namens Fred beschäftigt. Fred verfügt über ein Windows 2000 Netzwerkprofil mit der Bezeichnung FRED, ein Benutzerprofil auf SYSTEM1 mit der Bezeichnung LARRY mit PASSWORD *NONE und ein drittes Profil auf SYSTEM2 mit der Bezeichnung MOE, ebenfalls mit PASSWORD *NONE. Wenn Fred sich morgens auf seinem Laptop anmeldet, tut er das mit der Benutzer-ID FRED. Ein Verzeichnis des Systems SYSTEM2 („RemDir“), das zwei Streamfiles (MoeAccess und NoMoeAccess) enthält, ist auf SYSTEM1 unter Verwendung von „/other“ als mount point referenziert (mounted).

Nachdem Fred sich als FRED an seinem Laptop angemeldet hat, startet er den iSeries Navigator und klickt auf SYSTEM1. Dort wird er umgehend als LARRY angemeldet, ohne sich neu authentifizieren zu müssen. Nun klickt Fred auf IFS, root und „other“ auf der linken Seite der Anzeige iSeries Access for Windows. LARRY verfügt über die private Berechtigung *USE für das Verzeichnis „/other“ auf SYSTEM1, damit authentifiziert QFileSvr400 ihn nun mittels Kerberos gegenüber SYSTEM2. QFileSvr400 prüft die Authentifizierung und bildet die Kerberos Identität mittels EIM auf MOE ab.

Die beiden Dateien MoeAccess und NoMoeAccess werden nun im iSeries Navigator angezeigt. MOE verfügt über *ALL Berechtigung für die Datei MoeAccess und *USE Berechtigung für die Datei NoMoeAccess. Klickt Fred nun auf die Datei MoeAccess und benennt sie um, so funktioniert das einwandfrei. Klickt er aber auf die Datei NoMoeAccess und versucht, auch diese Datei umzubenennen, schlägt diese Operation fehl, da Fred nicht über die entsprechende Berechtigung verfügt. Dies alles geschieht, obwohl sich Fred nur ein einziges Mal mit seiner Windows 2000 Benutzer-ID auf seinem Laptop angemeldet hat.

OS/400 Konfiguration für Single Sign-On

Um einem System die Teilnahme in einer EIM SSO Umgebung zu ermöglichen, ist eine Konfiguration erforderlich, die dem System mitteilt, welchen Kerberos realm (Kerberos Server) es verwenden soll. In V5R2 steht über den iSeries Navigator ein Assistent für die Konfiguration des Network Authentication Service (NAS) zur Verfügung, mit dessen Hilfe sich diese Aufgabe relativ einfach erledigen lässt.