Windows Integration

von Tino Truppel

Agenda

- Ziele einer Integration von Windows in bestehende UNIX-Netzwerke
- Zugriff auf NFS-Freigaben
- Authentifikation an einem UNIX-KDC
- Authentifikation an einem Windows-KDC
- Einrichten eines Cross Realm Trusts

Agenda

- Ziele einer Integration von Windows in bestehende UNIX-Netzwerke
- Zugriff auf NFS-Freigaben
- Authentifikation an einem UNIX-KDC
- Authentifikation an einem Windows-KDC
- Einrichten eines Cross Realm Trusts

Ziele einer Integration

- Administration eines heterogenen Netzwerkes mit zentraler Benutzerverwaltung
- einfache Benutzbarkeit aus Nutzersicht:
  - Single-Sign-On Lösung
  - Jeder Benutzer besitzt genau ein Passwort
  - Daten des Nutzer werden konsistent und nicht doppelt gehalten
- Sicherheit

Situation

- ASG-Platform.org:
  - Ein bestehendes UNIX-Netzwerk mit NIS/NFS Benutzerverwaltung
- Funktionsfähiges Kerberos:
  - Läuft auf einem Debian Linux
- AFS Service vorhanden:
  - Läuft auch auf einem Debian Linux
- Meine Aufgabe:
  - Windows XP Clients sollen auf diese Dienste zugreifen können

Agenda

- Ziele einer Integration von Windows in bestehende UNIX-Netzwerke
- Zugriff auf NFS-Freigaben
- Authentifikation an einem UNIX-KDC
- Authentifikation an einem Windows-KDC
- Einrichten eines Cross Realm Trusts

Zugriff auf NFS-Freigaben (1/2)

- Was ist NFS:
  - Network File System
  - von Sun Microsystems entwickeltes Protokoll
  - Zugriff auf Dateien über ein Netzwerk ermöglicht
- Umsetzung:
  - Installation von Services for UNIX (SFU)
  - Zugriff auf das NFS-Share:
    - **`Mount tb0.asg-platform.org: /home/%USERNAME% H:`**
  - Einrichten einer Batch-Datei im Autostart

Zugriff auf NFS-Freigaben (2/2)

- Vorteile:
  - Einfach einzurichten
  - Es wird kein Windows Server benötigt
- Nachteile:
  - Auf Windowsseite keine zentrale Benutzerverwaltung
  - Unsicher
  - Es kann nur dieser Service genutzt werden

Agenda

- Ziele einer Integration von Windows in bestehende UNIX-Netzwerke
- Zugriff auf NFS-Freigaben
- Authentifikation an einem UNIX-KDC
- Authentifikation an einem Windows-KDC
- Einrichten eines Cross Realm Trusts

Authentifikation an UNIX-KDC (1/3)

(eines Windows Einzelplatzrechners)

- Dem Windowsclient das Realm bekanntmachen:
  - Geschieht mit Hilfe des ksetup.exe Tools:
    - **`KSetup /SetRealm ASG-PLATFORM.ORG`**
    - **`KSetup /AddKdc ASG-PLATFORM.ORG seidel.asg-platform.org`**
    - **`KSetup /SetComputerPassword password`**
    - **`KSetup /MapUser * *`**

Authentifikation an UNIX-KDC (2/3)

- Einrichten von Hostprincipals im KDC:
  - **`kadmin: ank -e des-cbc-crc:normal host/livny.asg-platform.org`**
- Windows nicht voll kerberoskompatibel, da nur diese einfache Verschlüsslungsmethode unterstützt wird

Authentifikation an UNIX-KDC (3/3)

- Vorteile:
  - Sicherer
  - Nutzung von sämtlichen Services möglich, welche von Kerberos unterstützt werden
  - Kein Windows Server nötig
- Nachteile:
  - Keine zentrale Benutzerverwaltung
  - Auf jeden Client muss jeder Benutzer lokal vorhanden sein

Agenda

- Ziele einer Integration von Windows in bestehende UNIX-Netzwerke
- Zugriff auf NFS-Freigaben
- Authentifikation an einem UNIX-KDC
- Authentifikation an einem Windows-KDC
- Einrichten eines Cross Realm Trusts

Authentifikation an Windows-KDC

(kurzer Einschub)

- Einrichten eines Active Directory (auf einem Windows 2003 Rechner)
- Enthält bereits ein Kerberos
- Der Zugriff ist nativ
- Clients treten der Domäne bei

Agenda

- Ziele einer Integration von Windows in bestehende UNIX-Netzwerke
- Zugriff auf NFS-Freigaben
- Authentifikation an einem UNIX-KDC
- Authentifikation an einem Windows-KDC
- Einrichten eines Cross Realm Trusts

Cross Realm Trust einrichten (1/3)

- Was ist ein Cross Realm Trust:
  - Bedeutet Vertrauensstellung zwischen zwei Kerberosrealms
  - Nutzer aus diesem Realm kann Services vom fremden Realm nutzen und/oder andersherum
- Arten eines Cross Realm Trusts:
  - Unidirektional oder bidirektional
  - Transitiv oder nicht-transitiv

Cross Realm Trust einrichten (2/3)

- Einrichten des Windows 2003 Servers:
  - KSetup ausführen
  - Einrichten des Trusts
  - Mapping der Nutzernamen
- Einrichten des Linux KDCs:
  - **`kadmin: ank -e des-cbc-crc:normal krbtgt/ASG-PLATFROM.ORG@WIN2003.ASG-PLATFORM.ORG`**
  - **`kadmin: ank -e des-cbc-crc:normal krbtgt/WIN2003.ASG-PLATFORM.ORG@ASG-PLATFROM.ORG`**

Cross Realm Trust einrichten (3/3)

- Vorteile:
  - Halbwegs zentrale Benutzerverwaltung
  - Zugang zu netzweite Services
  - Sicher
- Nachteile:
  - Es wird Windows 2003 Server benötigt
  - Nutzer müssen zweimal angelegt werden

Quellen

- Microsoft:
  - Windows Hilfe (für SFU Unterstützung)
  - microsoft.com/windows2000/techinfo/howitworks/security/kerbint.asp (für Cross Realm Trusts)
- Kerberos Manual:
  - web.mit.edu/kerberos/www/
- Single-Sign-on am Beispiel TFH Wildau:
  - wi-bw.tfh-wildau.de/~pboettch/home/sso/index.html

Vielen Dank

Gerne beantworte ich weitere Fragen!