Zentrale Benutzerverwaltung für Studenten, Authentifizierungs-Server

LDAP-Authentifizierungs-Server (mit OpenSource)

August 2004, Best-Practice-Papier zum IT-Sicherheitskonzept der FH Gelsenkirchen.

1 Ziele

Mit Hilfe von einfachen, kostengünstigen Mitteln soll eine zentrale Benutzerverwaltung sowie Benutzerauthentikation ermöglicht werden. Als „Benutzer" stehen zunächst Studenten im Vordergrund, allerdings soll das System durch andere Benutzergruppen erweiterbar sein.

- kein Single-Point-Of-Failure, möglichst dezentrale Struktur
- pool-spezifische Zugangskontrollfunktionen
- einfaches, automatisiertes Einfügen von neuen Benutzern/Studenten

2 Voraussetzungen

- Schnittstelle zu LDAP muss von den angebotenen Diensten vorhanden oder installierbar sein

3 Struktur

3.1 LDAP-Master

Zentrale Datenbank für die Verwaltungs- und Authentikationsdaten ist der LDAP-Master. Hier werden neue Benutzer eingefügt und Änderungen (z.B. Passwortänderungen) durchgeführt. Auf dem LDAP-Master müssen die Daten gespeichert, die für alle angeschlossenen Proxies gleich sind. Dies sind in der Regel, eine eindeutige Benutzeridentifikation (User ID), ein Passwort sowie der Name des Benutzers.

Der LDAP-Master kann mit einem LDAP-Secondary ausfallsicherer gemacht werden. (Open)LDAP bringt hier Mechanismen mit, um dies auf Datenbank-Basis zu ermöglichen.

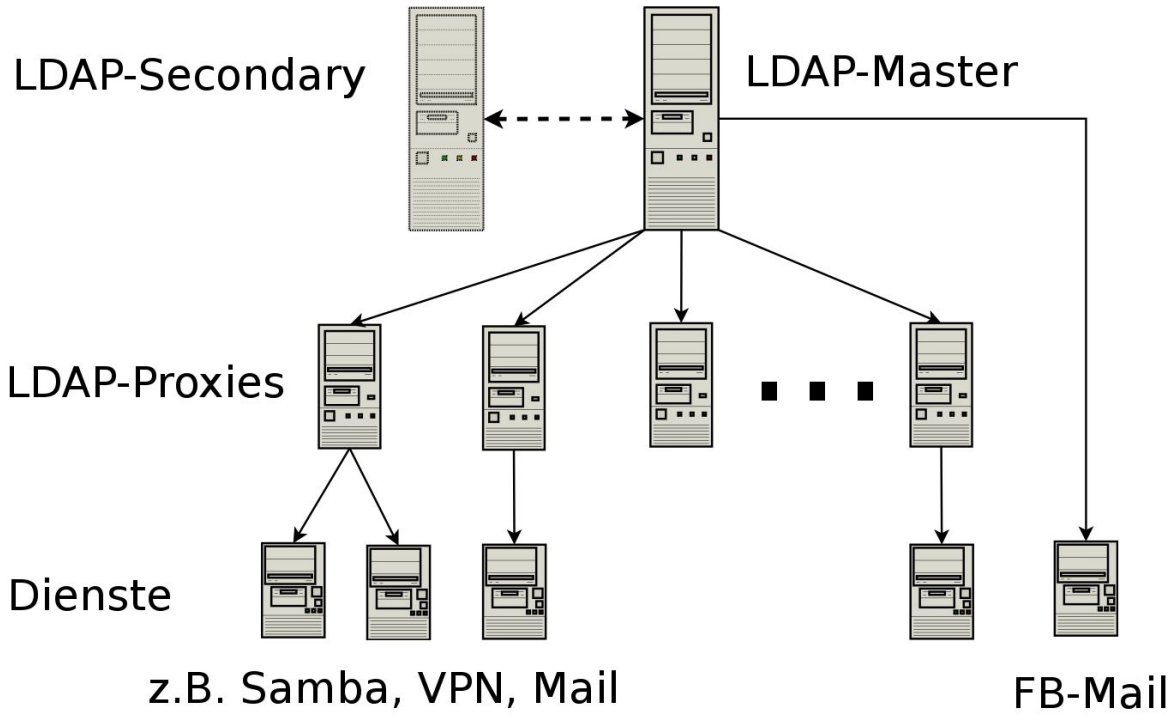

Abbildung 1 Die Struktur der LDAP-basierten Verwaltung

3.2 LDAP-Proxies

Damit ein Single-Point-Of-Failure vermieden und die Last verteilt wird, authentifizieren die angebotenen Dienste nicht direkt gegen den LDAP-Master, sondern gegen zwischengelagerte LDAP-Proxies. Bei einem Ausfall des LDAP-Masters ist der laufende Betrieb nicht gefährdet, denn die Proxies können weiterhin Benutzer authentifizieren, allerdings können keine neuen Benutzer hinzugefügt werden oder Daten geändert werden (z.B. Passwortänderungen).

Die Proxies sind Stellvertreter für den LDAP-Master, wenn es um Authentikation geht. Im FB Informatik gibt es ungefähr pro PC-Pool einen Proxy.

Des weiteren können auf den Proxies aber auch zusätzliche Felder zur Zugangskontrolle eingerichtet werden. So kann z.B. ein Student durch Setzen eines Feldes in der LDAP-Datenbank sofort von der Nutzung eines PC-Pools temporär ausgeschlossen werden.

Die LDAP-Proxies synchronisieren ihren Datenbestand in bestimmten Abständen durch Polling mit dem LDAP-Master. Hierbei werden Änderungen immer nur eine Richtung, vom Master zum LDAP-Proxy übertragen. Die Synchronisierung erfolgt im FB Informatik per Perl-Skript und kann über eine SSL/TLS-Verbindung sicher getunnelt werden, sodass die Daten nicht mitgelesen oder modifiziert werden können.

Die LDAP-Proxies sind nicht unbedingt notwendig, sondern optionale Komponenten und können unter Verzicht auf die Redundanz und Lastverteilung außen vor gelassen werden. Hierbei ist jedoch zu bedenken, dass mit dem Ausfall des LDAP-Masters auch kein von LDAP-abhängiger Dienst mehr authentifizieren kann. Bei Verwendung von Proxies ist auch bei einem Ausfall des LDAP-Masters der laufende Betrieb weiterhin möglich.

3.3 Dienste

Die Dienste müssen entweder bereits eine Schnittstelle zu LDAP besitzen oder eine

Schnittstelle zu einem generischen Authentikationsdienst (z.B. PAM unter GNU/Linux). Bei vielen Dienste unter GNU/Linux ist dies vorhanden oder relativ einfach per Skript nachrüstbar.

Zur Zeit sind lediglich passwortauthentifizierte Dienste möglich. Es ist aber auch denkbar, dass die LDAP-Datenbank um ein Zertifikatseintrag o.ä. erweitert wird, um mit Hilfe von Zertifikaten zu authentifizieren.

3.4 Einfügen von neuen Studenten

Neue Studenten können sich zur Zeit über eine Anmelde-Station im PC-Pool selbst anmelden. Hierzu müssen sie ihren Studenten-Ausweis auf den Scanner legen und einige Daten (Name, Vorname, Email-Adresse, etc.) eingeben.

Die Anmeldung wird dann per Email an den PC-Pool-Verwaltenden geschickt. Die entsprechende Person verifiziert die eingegebenen Daten sowie den Scan des Studenten-Ausweises und gibt den Anstoß, dass die Daten in die LDAP-Datenbank übernommen werden können. Das Passwort wird automatisch zufällig gewählt und dem Studenten per Email zugeschickt.

Neue Accounts werden nur auf dem LDAP-Master hinzugefügt. Die Proxies synchronisieren ihren Datenbestand mit dem des Masters nach einem beliebig definierten Zeitintervall.

3.5 Passwortänderungen

Die Studenten können ihr Passwort über ein Web-Interface ändern. Das neue Passwort wird auf „Passworttauglichkeit" überprüft und kann falls gewünscht nur nach erfolgreicher Prüfung als neues Passwort zugelassen werden.