Autentifikacijski sustavi i baze podataka

LDAP

Uvod

- Što je potrebno da utvrdimo da li netko ima **pravo** pristupa?
  - Autentifikacija (username + password)
  - Autorizacija (“što mogu” – dodjela prava)

- Gdje možemo spremati podatke o korisnicima?
  - Lokalno (na računalu/poslužitelju)
  - Unutar neke domene (npr. unutar student.hr domene)
  - Globalno (npr. korištenje facebook.com korisničkih podataka za cca 60.000 web stranica)
    - Popis: https://trends.builtwith.com/websitelist/Facebook-Login-Button

Čemu služe Imenički sustavi (1)

- Za spremanje korisničkih podataka
- Za spremanje korisničkih prava
- Limitiran pristup (ne želimo svoje podatke naći na “Internetu”)
  - Imenik mora aplikaciji dozvoliti pravo pristupa čitanja podataka za potrebe:
    - Autentifikacije (utvrđivanje korisnika)
    - Autorizacije (koja prava nasljeđujem ili su opisana u imeniku)
- Za spremanje podataka o korisniku koristimo (neku) bazu podataka

Čemu služe Imenički sustavi (2)

- Gdje se što na mreži nalazi
  - Organizacija
  - Osoba
  - Resurs (npr. Printer, dokumenti, e-mail…)

- Što mi npr. treba da pronađem e-mail kolege iz firme?
  - Pokušaj i pogodak
  - Pretraga imeničkog sustava

Primjeri imeničkih sustava

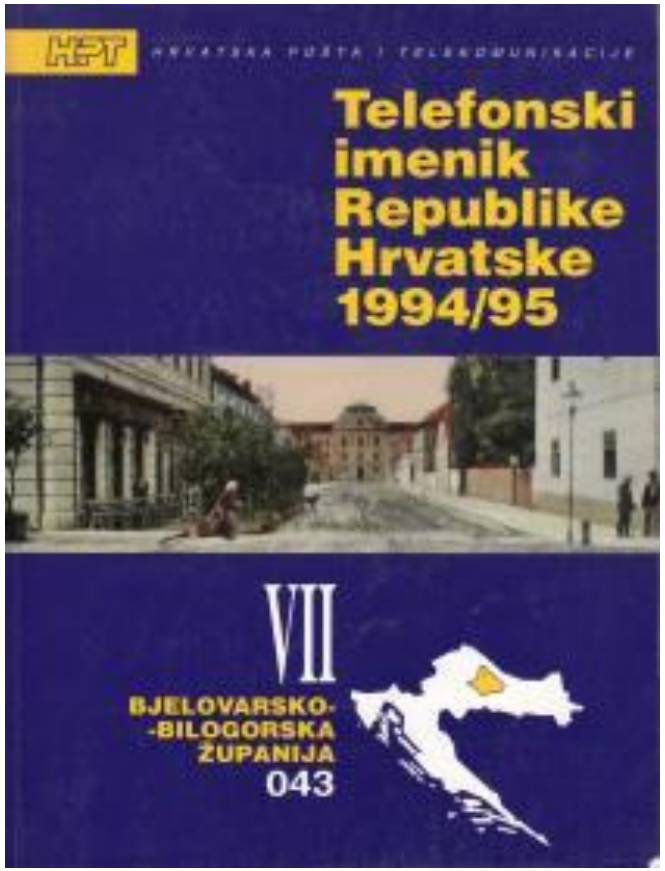
- 389 Direcrory Server – RedHat
  - FreeIPA (open-source verzija)
- Active Directory – Microsoft
- Apple Open Directory – za potrebe MacOSx
- Oracle Internet Directory
- OpenDS – Sun Microsystems
- IBM Tivoli Directory
- OpenLDAP – razvoj pokrenulo “*University of Michigan*” (open-source)
- Lotus Domino – IBM/HCL Technologies
- …

LDAP

- Lightweight Directory Access Protocol
  - RFC 4511 (verzija 3)
  - Industrijski standard
  - Otvoren, vendor-neutralan
- Opisuje način pristupa distribuiranim imenicima preko IP mreže i koristi
- **Izraz LDAP** se **ne** koristi za bazu podataka već **protocol** kako razgovarati sa imeničkom bazom podataka (upit/pretraživanje)
- **LDAP server** – program koji implementira imeničku bazu podataka koji može razgovarati sa aplikacijama koji te podatke trebaju putem LDAP protokola

LDAP povijest

- X.500 protocol (ITU standard)
- Nastao kao potreba za spremanje telefonskih brojeva
  - Ime i Prezime
  - Telefonski broj
- Razvojem Internet mreže korisnici koriste:
  - Država
  - Posao
  - Radno mjesto
  - E-mail



Prvi primjer zapisa:

cn=Pero Perić, ou=Marketing, ou=Dizajner, o=Firma d.o.o., c=Hrvatska

X.500/LDAP

- cn=Pero Perić, ou=Marketing, ou=Dizajner, o=Firma d.o.o., c=Hrvatska

- ***Što ako je korisnik promjenio radno mjesto?***
- ***Što ako je korisnik promjenio prezime?***

- Današnji imenici koriste DN (Distinguish name)
  - “Široki opis korisnika”
  - Uvođenje UIDa (User ID)
  - Uvođenje schema
  - **U imenicima nisu samo ljudski korisnici!**

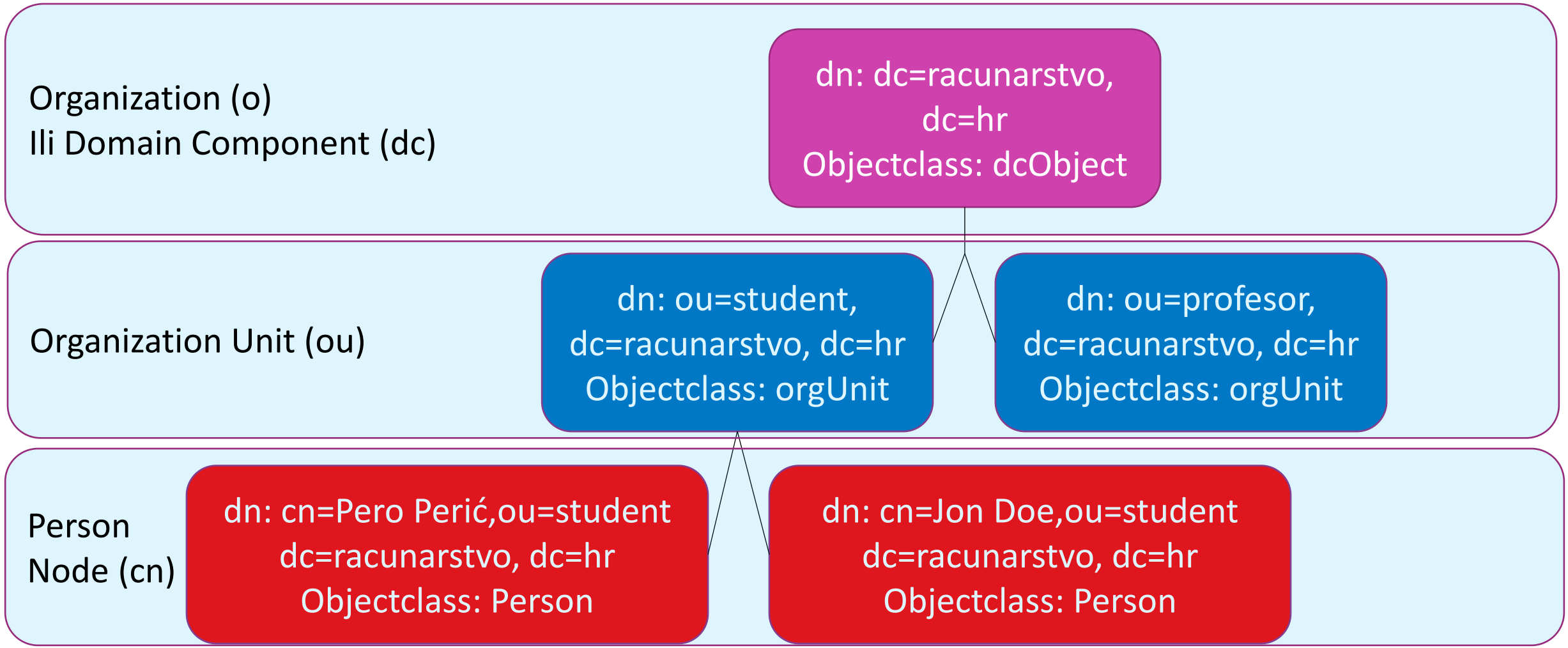
LDAP zapis (1)

- Hijerarhijski zapisi (drvo) – Directory Information Tree
  - Definiran schemom
- DN
  - Najvažniji zapis o **identitetu** (u čemu se sve razlikuje od drugih tj. u čemu je jedinstven)
- Atributi
  - Dodatni opisi korisnika
  - Mogu se prilagoditi
- Objektne klase
  - Definiraju koji atributi se nalaze u kojem objektu

LDAP zapis (2)

- Što može biti identitet:
  - Korisnici
  - Računala i računalna oprema
  - Virtualna računala
  - Grupe

LDAP zapis (3)


Organization (o)
Ili Domain Component (dc)
dn: dc=racunarstvo, dc=hr
Objectclass: dcObject
Organization Unit (ou)
dn: ou=student, dc=racunarstvo, dc=hr
Objectclass: orgUnit
dn: ou=profesor, dc=racunarstvo, dc=hr
Objectclass: orgUnit
Person Node (cn)
dn: cn=Pero Perić,ou=student dc=racunarstvo, dc=hr
Objectclass: Person
dn: cn=Jon Doe,ou=student dc=racunarstvo, dc=hr
Objectclass: Person

LDAP

- TCP/UDP portovi 389 ili 636
- LDAP komande nad zapisima u bazi podataka:
  - Search (pretraži)
  - Add (dodaj)
  - Modify (promjeni)
  - Delete (izbriši)
- Binarni protocol (u pravilu nije kriptiran) – čojvek ne može pročitati informaciju (*ne šalje se text file*)
- Za sigurnu komunikaciju dodatno koristi “*sigurnosne tunele*” TLS/SSL

LDAP aplikacije (otvorenog koda)

- Serveri: OpenLDAP, FreeIPA…
- CLI aplikacije: ldapsearch
- Front-end management: phpLDAPadmin…

Windowsi i LDAP

- Microsoft podržava LDAP protocol
- Windows računala mogu koristiti vanjske autentifikacijske LDAP servere (nije potreban AD za dodavanje računala u Domenu)
- Primjer: korištenje pGina za autorizacijske scheme unutar Windowsa
    - Active Directory je podržan od Microsofta

Active Directory vs OpenLDAP

- AD je isključivo na Windows platformi, OpenLDAP radi u heterogenoj okolini
- AD koristi više protokola za autentifikaciju korisnika (LDAP, Kerberos, NTML, LAN Manager…), dok OpenLDAP koristi samo LDAP
- OpenLDAP zahtjeva iskusnije sistemce
- OpenLDAP je besplatan, AD se plaća

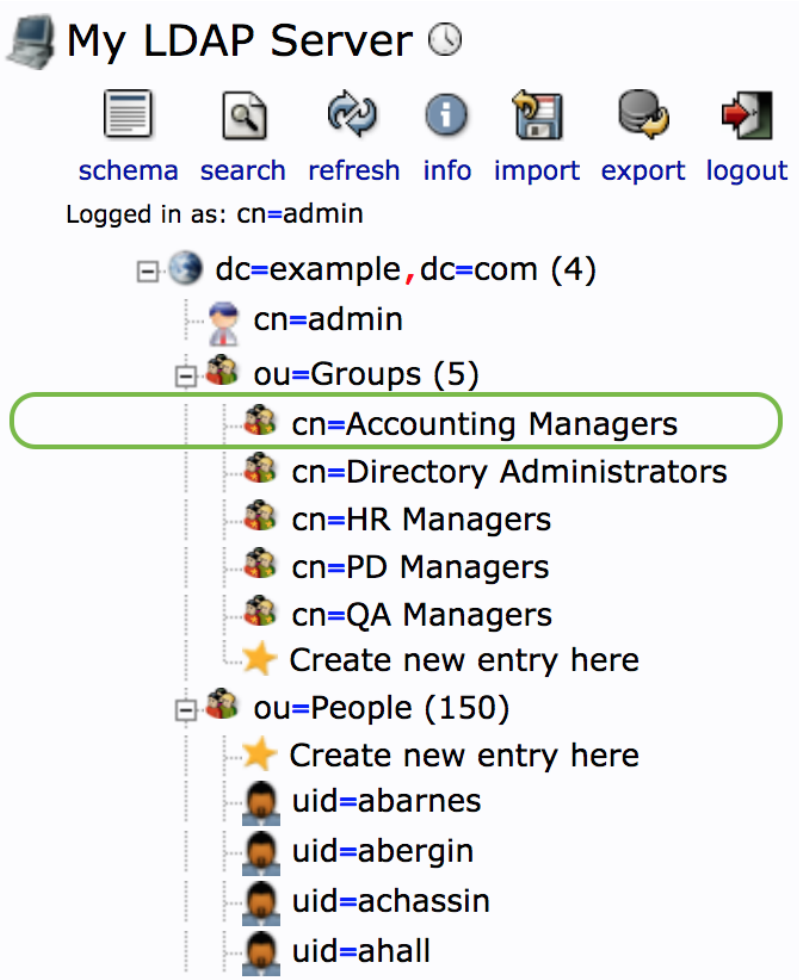
Autentifikacija pomoću LDAPa

- U bazi podataka se nalazi i korisnička zaporka (password)
- Metode za autentifikaciju preko mreže:
  - PLAIN
  - Kerberos
  - SASL (Simple Authentication and Security Layer)
- Rezultat uspješne autentifikacije je povratna informacija: **LDAP_SUCCESS** – korisnički podaci su ispravni

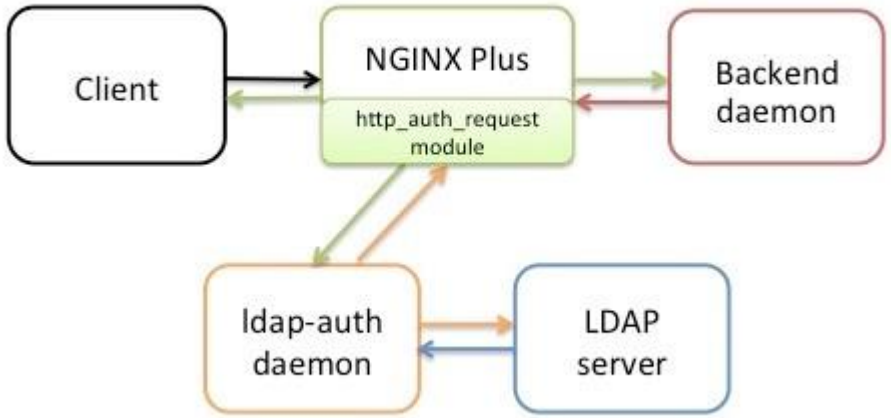
- Primjer: Spajanje na Infoeduca stranicu
  - Stranica prosljeđuje username i password preko LDAP upita na Imenički sustav (OpenLDAP) i čeka povratnu informaciju
  - Prednost: Infoeduka ne treba voditi brigu o ispravnim podacima korisnika ali ih koristi

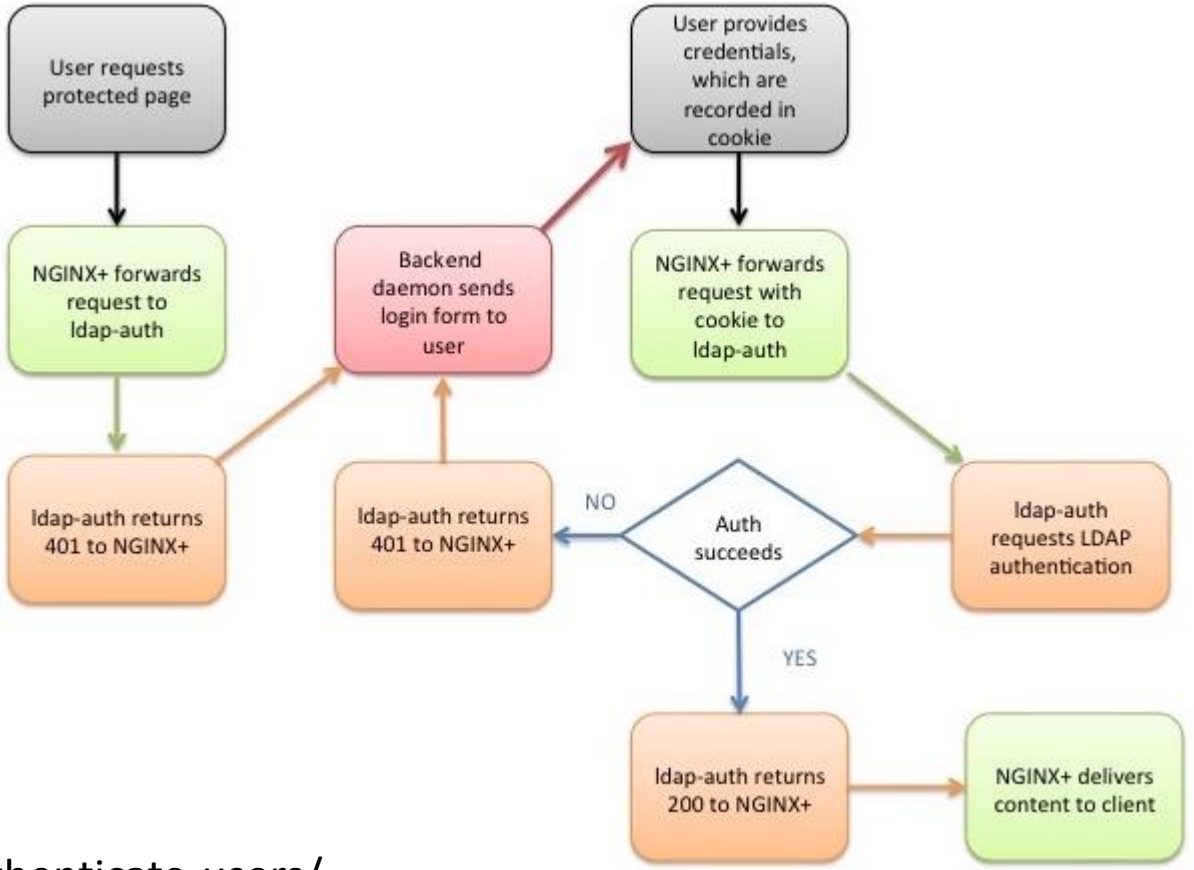
Autorizacija pomoću LDAPa

- Tko smije pristupati kojem servisu ili resursu
- Primjeri:
  - Ako je ou atribut == IT i cn == admin -> dozvoli korisniku admin ovlasti
  - Ako je **ou** atribut grupe == računovodstvo -> dozvoli čitanje računovodstvenih izvještaja



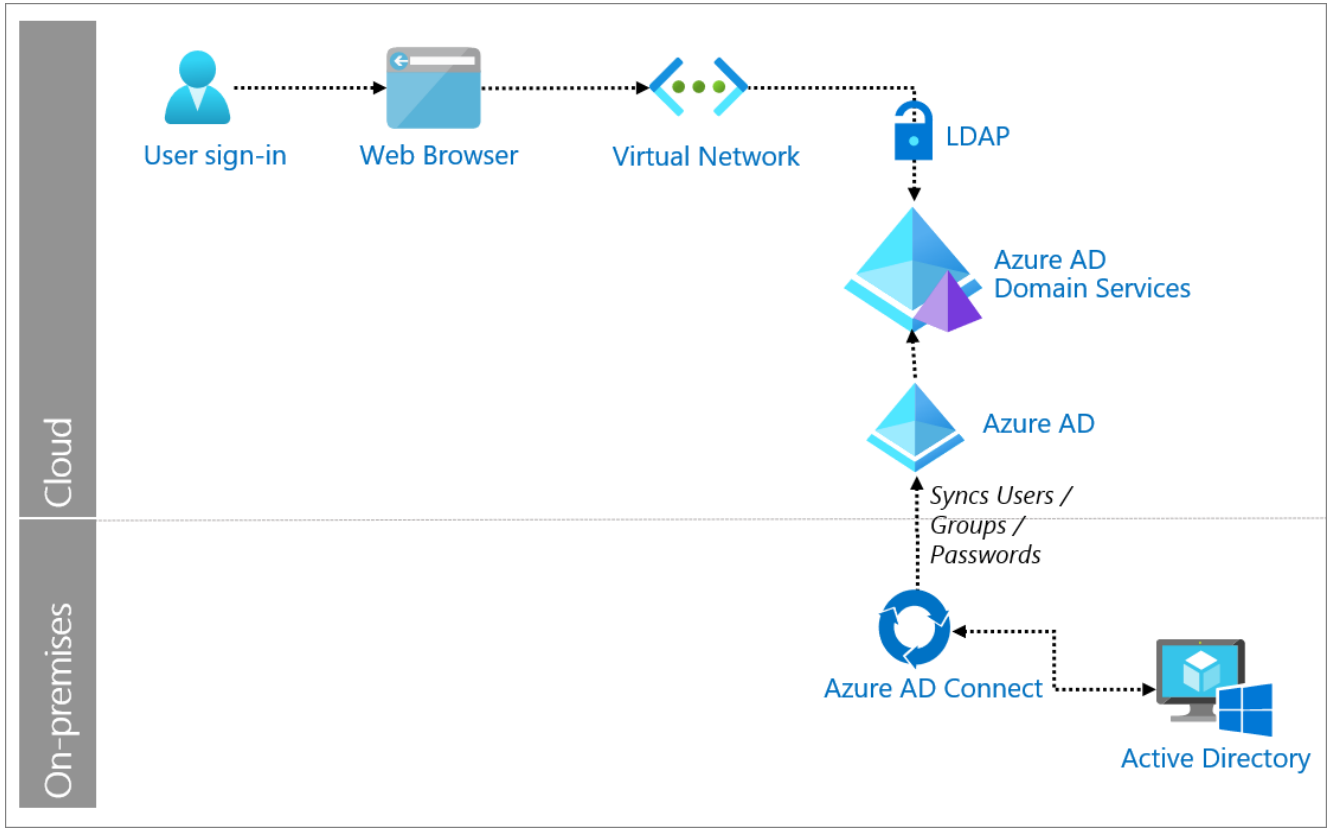
Primjer korištenja LDAPa (Web login)





Izvor: https://www.nginx.com/blog/nginx-plus-authenticate-users/

LDAP autentifikacija sa Azure Active Directory



Izvor: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/auth-ldap

Zapis studenta na VUA

- Koji podaci se zapisuju:
  - https://www.aaiedu.hr/sites/default/files/content_files/docs/AAI%40EduHr-hrEduSheme-2010-v1.3.1.pdf
- Što AAI@edu.hr zna o meni:
  - https://moj.aaiedu.hr/
- AAI@edu.hr usluge:
  - Spajanje na edukacijske portale
  - Pretrage baza podataka
  - Eduroam – spajanje na bežičnu mrežu SSID: Eduroam bilo gdje u svijetu

LDAP protocol vs RADIUS protocol

- Oba služe za autent. & auth. korisnika na mrežne resurse
- Oba su standardi
- Oba imaju Open-source implementacije
- LDAP je primarno stvoren za autentifikaciju na neki system ili aplikaciju
- RADISU je kreiran za spore mrežne veze (dial-up) ali se danas primarno koristi za autentifikaciju na **mrežnu infrastrukturu** (npr. spajanje računala na Internet, VPN, routers…)
  - RADIUS protocol može “pričati” sa imeničkim bazama – istim onima koje i LDAP koristi

Demo

- FreeIPA
  - Install
  - Korištenje

Pitanja

?

Hvala na pažnji!