AAI@EduHr, AOSI i LDAP savjeti i trikovi

Matko Kosmat | 30 ožujka, 2026

Ova online knjiga je skup pojedinačnih članaka objavljenih kao pomoć sistemcima u konfiguraciji i korištenju AAI@EduHr, AOSI i LDAP sustava i servisa.

Za autentikaciju različitih servisa putem LDAP-a mogu se koristiti dva modula: **pam_ldap** i **pam_radius**. Preporuka AAI@EduHr službe je uporaba modula pam_radius, pa će ovaj članak biti baziran na njemu.

Način rada u ovom slučaju je posredan, jer pam_radius kontaktira RADIUS server, koji zatim komunicira s LDAP serverom.

Uz pretpostavku da se radi o Debian Linuxu, potrebno je instalirati paket libpam-radius-auth koji donosi potreban PAM modul. Instalacija je standardna:

U konfiguraciji FreeRADIUS-a prijavite poslužitelja kao klijenta:

U našem slučaju je klijent na lokalnom računalu (localhost)

Ovaj secret se treba prenijeti i u konfiguraciju pam_radius-a u datoteci /etc/pam_radius_auth.conf:

Time smo obavili predradnje za autentikaciju servisa preko RADIUS-a. Konfiguracijske datoteke PAM-a nalaze se u direktoriju /etc/pam.d/.

Ako želite sve servise autenticirati preko RADIUS-a, u datoteci /etc/pam.d/common-auth, bez diranja ostalih datoteka, zakomentirajte redak:

i dodajte:

Time smo postigli da se autentikacija korisnika obavlja preko RADIUS servera, a tek u slučaju neuspješne autentikacije pita se pam_unix (odnosno traži unos zaporke navedene u datoteci /etc/shadow). To je dobro, jer će se sistemac moći prijaviti na poslužitelj i u slučaju ispada RADIUS-a ili LDAP-a.

Svaki servis ima svoju konfiguracijsku datoteku i može se zasebno podešavati. Na primjer, za Secure shell u /etc/pam.d/ssh zakomentirajte redak:

i dodajte dva nova:

U /etc/pam.d nalazi se konfiguracija i za druge servise. Na isti način možete unijeti i konfiguraciju na primjer za ftp, imap, pop itd.

Nedavno sam rješavao neobičan slučaj korisnika koji se spaja na Internet od kuće preko meže kablovskog operatera. Korisnik je sklopio ugovor s Bnetom i podesio kućni router da pri spajanju obavi autentikaciju koristeći elektronički identitet koji je dobio na ustanovi.

Korisnik se požalio da mu je iznenada uskraćena usluga, a da nije ništa mijenjao u konfiguraciji routera. Pri pokušaju spajanja dobije poruku: ***PPTP server not found on specified address***. Zvao je Bnetovu podršku, gdje mu je rečeno da će oni proučiti problem i da će ga netko nazvati. Dani su prolazili, nitko nije zvao. Nazvao je ponovo Bnet, ovog puta je operater bio neljubazan, drsko je odgovorio da je kod njih sve u redu i neka se izvoli obratiti CARNetu. Čak je tvrdio kako on vidi da je router dobio IP adresu, što nije bilo točno, verojatno je vidio adresu dodijeljenu modemu.

Korisniku sam sugerirao da se pokuša ulogirati na web sučelju LDAP servisa na ustanovi, kako bi provjerio da li su mu ispravni korisničko ime i zaporka. Sve je prošlo kako treba, a isto korisničko ime i zaporka ispravno su uneseni u konfiguraciju kućnog routera. Dakle problem je u nečem drugom.

U logovima koje radius zapisuje na Linux serveru ustanove pronađeni su brojni zapisi koji pokazuju da korisnikov router svake sekunde obavlja autentikaciju:

Sat Nov 5 11:33:50 2011 : Auth: Login OK: [korisnik@domena.hr] (from client aaics2 port 0)
Sat Nov 5 11:33:51 2011 : Auth: Login OK: [korisnik@domena.hr] (from client aaics2 port 0)
Sat Nov 5 11:33:52 2011 : Auth: Login OK: [korisnik@domena.hr] (from client aaics2 port 0)
Sat Nov 5 11:33:53 2011 : Auth: Login OK: [korisnik@domena.hr] (from client aaics2 port 0)
Sat Nov 5 11:33:54 2011 : Auth: Login OK: [korisnik@domena.hr] (from client aaics2 port 0)

Dakle autentikacija je uspjela, ali zašto router ne dobije IP adresu iz CARNetova adresnog prostora, nego uzaludno pokušava ponovo?

Zatražio sam pomoć AAI@Edu.Hr tima sa Srca. Njihova sugestija uputila me u pravom smjeru. Pružatelji usluga mogu osim korisničkog imena i zaporke provjeravati i neke druge atribute iz LDAP imenika, na primjer datum isteka elektroničkog identiteta! I zaista, korisnik je i dalje imao otvoren račun, ali je u polje **Datum isteka temeljne povezanosti** bio upisan datum koji je već prošao! Korisnik nije student, pa nije dobio račun na godinu dana, dok ne upiše slijedeću godinu. LDAP administrator upisao je proizvoljan datum, koji je u vrijeme otvaranja računa izgledao daleko u budućnosti, ali vrijeme nemilosrdno teče pa je daleka budućnost neprimjetno postala prošlost.

U polje **Datum isteka temeljne povezanosti** moguće je za djelatnike u stalnom radnom odnosu upisati vrijednost **NONE**, obavezno velikim slovima. LDAP administrator će si na taj način olakšati posao, jer neće morati provjeravati kojim je korisnicima isteklo važenje elektroničkog identiteta.

Na kraju, nazvali smo Bnetovu korisničku podršku i objasnili da uzrok problema može biti istek važenja elektroničkog identiteta, tako da ubuduće mogu CARNetove korisnike uputiti da u svojoj ustanovi provjere taj podatak. Ovog je puta operater bio vrlo ljubazan i zahvalio na korisnoj informaciji. Problem riješen.

Jedan od češćih problema nakon uspješne migracije i importa podataka iz starog LDAP-a u novu imeničku shemu AAI@EduHr, jest da se ne možete prijaviti kao administrator u AOSI aplikaciju.

Čest je razlog jednostavno zaboravljena zaporka, ali se može dogoditi (kao što je bio slučaj na pojedinim institucijama) da ste jednostavno "zaboravili" importirati administratora, odnosno definirati određenog korisnika kao administratora.

Problem se može riješiti u nekoliko koraka na jednostavan način, uz pomoć jednog od vaših korisnika.

Sve što vam treba je korisnik i njegova zaporka (djelatnik ustanove ili student kojeg osobno poznajete), pod uvjetom da postoji u novoj shemi i da zna svoju zaporku. Njegovu korisničku oznaku upišite u /etc/aosi/valid_user (ne zaboravite na kraju enter!), dodajte još svoj username i snimite datoteku.

Restartajte aplikaciju AOSI:

Korisnik je sad (privremeno) postao administrator. Prijavite se kao taj korisnik, možete ga zamoliti da se pred vama ulogira. Pronađite sebe kao običnog korisnika i odmah promijenite zaporku. Ako Vas nema u bazi, dodajte se (ista korisnička oznaka koju ste si upisali u valid_user, pravilno popunite sva polja koja se traže). Odjavite se sa sustava i ponovo prijavite, ali sad pod svojim korisničkim imenom i zaporkom, te unesite u LDAP bazu dodatne administratore.

Nakon toga treba obrisati kolegu, privremenog admina, iz valid_user datoteke. Prije restartanja AOSI aplikacije, upišite u nju vaše nove administratore (održavatelje baze), koje ste u prethodnom koraku unijeli u bazu, kako bi se izbjegli slični slučajevi i olakšalo administriranje u slučaju vašeg odsustva.

Pri instalaciji produkcijskih paketa za AAI@EduHr primijetili smo da neki imaju nepravilno kriptirane lozinke u LDAP konfiguracijskoj datoteci (rootpw linija u /etc/ldap/slapd.conf).

Naime, prije je administratorska lozinka bila i u datoteci slapd.conf i u LDAP bazi. Moguće je da je lozinka u slapd.conf bila nepravilno kriptirana, a u bazi ispravno. Kako se baza obrisala zbog inicijalizacije potpuno nove baze s novom shemom, ostala je samo nepravilno kriptirana lozinka u slapd.conf.

Naredbom:

može se vidjeti kako kriptirana lozinka izgleda. Ispravan izgled je (npr.):

Ispravan kriptirani string kreiramo naredbom slappasswd:

Zatim ga upišemo u slapd.conf i restartamo slapd:

Nakon toga možemo nastaviti s instalacijom openldap-aai-cn:

U sustavu AAI@EduHr administratorska se lozinka zapisuje na dva mjesta. Da bi sustav ispravno radio, treba je promijeniti na oba mjesta.

Prvo mjesto izmjene je u datoteci /etc/ldap/slapd.conf pod direktivom rootpw. Naredbom slappasswd generira se kriptirani niz znakova (string):

Zatim se u /etc/ldap/slapd.conf pod direktivom rootpw stavlja taj kriptirani string:

Da bi promjena sjela, treba restartati LDAP poslužitelj:

Drugo mjesto promjene je konfiguracija AOSI web servisa. To se najjednostavnije obavlja naredbom:

Paket će provjeriti lozinku i javiti ako je neispravno postavljena.

I to je to!

AOSI WWW sučelje podešeno je tako da mu se može pristupiti samo s CARNetove mreže (193.198.0.0/16 i 161.53.0.0/16). Time se štiti administratorsko sučelje kojim se dodaju/brišu korisnici u LDAP. Ako za rad kod kuće koristite uslugu nekog drugog davatelja usluga, onda je potrebno dodati i njihove adrese u pristupnu listu AOSI WWW sučelja. To se radi u datoteci /etc/apache/conf.d/aosi-www.conf.

U toj datoteci, na kraju, unutar bloka Directory, stoji:

Tu se doda još neka mreža u CIDR (Classless Inter Domain Routing) notaciji.

Npr, za MaxADSL:

Kada se naprave izmjene, treba restartati Apache web server:

Ako želite u potpunosti maknuti pristupne liste, obrišite (ili bolje zakomentirajte) gore navedeni odjeljak, i restartajte Apache web server.

Loša je strana uklanjanja pristupnih listi to što se bilo tko od bilo kuda može pokušati spojiti na administratorsko sučelje, te nekom brute force metodom pokušati doći do lozinke.

Ako dozvolite pristup s ADSL adresa, pratite u logovima da li su se pojavili pokušaji provale. Tada razmislite da li vam je pristup od kuće zaista potreban.