Autentifikácia v D2000

Autentifikáciou sa rozumie overenie identity užívatea, t.j. overenie, že užívate je ten, ktorý tvrdí, že je. Overenie identity obecne prebieha na základe nieoho, o užívate vie (prihlasovacie meno + heslo), o vlastní (prihlasovací USB token, osobná ipová karta so šifrovacím a identifikaným kúom PKI), prípadne nejakého jeho merateného biometrického znaku (odtlaok prsta, scan dúhovky).
Štandardne overuje meno a heslo užívatea v D2000 proces D2000 Server. V niektorých prípadoch je výhodné, aby overovanie identity užívatea bolo presunuté na doménu Windows, o umožní:

- používanie tých istých hesiel do D2000 ako do Windows domény (NTLM autentifikácia),
- používanie tých istých mien a hesiel do viacerých systémov D2000, pre ich zmenu staí zmeni heslo na jednom mieste - heslo do Windows (NTLM autentifikácia),
- automatické prihlásenie sa do D2000 bez zadávania mena a hesla iba na základe toho, že užívate je prihlásený do Windows domény (Kerberos autentifikácia),
- zabezpei prihlásenie užívatea do D2000 hardvérovo (prihlasovací USB token, osobná ipová karta so šifrovacím a identifikaným kúom PKI) tak, že sa takéto zabezpeenie použije na prihlasovanie sa užívatea do Windows a následne sa použije Kerberos autentifikácia na prihlásenie do D2000,
- zakázanie prihlásenia užívatea do D2000 nástrojmi pre správu užívateov v doméne Windows,
- nastavenie parametrov, ktoré musí spa heslo do D2000, nástrojmi pre správu užívateov v doméne Windows.

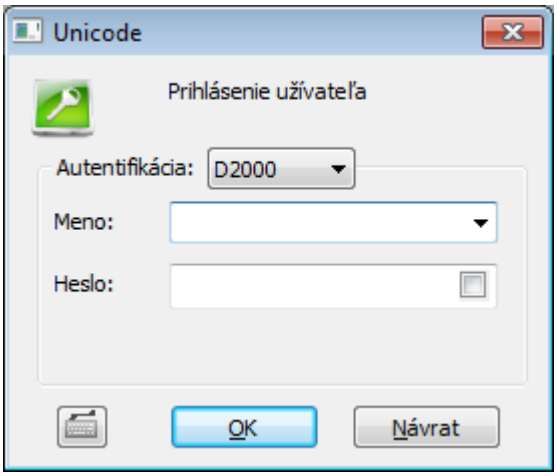
Poznámka pre platformy Linux a Raspberry PI: od verzie D2000 12.2.65 (patche z 27.5.2020 a novšie) je Kerberos autentifikácia dostupná aj na platformách Linux x64 a Raspberry PI. Na sfunknenie je nutné vykona nasledovné kroky:

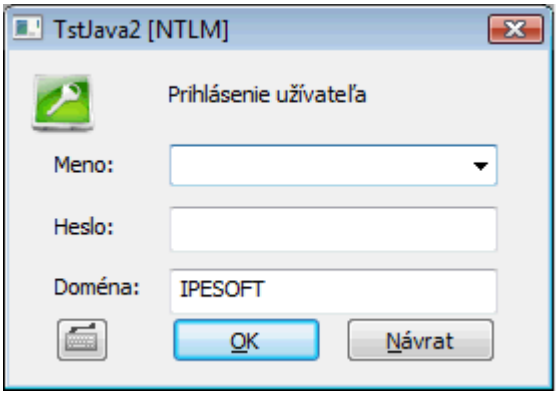
- zaradenie Linux/Raspberry PI servera do Windows domény
  (príkazom *realm join meno_domény*, napr *realm join IPSTEST.SK*)
- umožnenie prístupu D2000 Serveru (*kernel*) k súboru */etc/krb5.keytab*. Jednou možnosou je nakonfigurova spúšanie D2000 Servera pod užívateom *root*, inou - menej dramatickou - je nakonfigurovanie prístupových práv pre skupinu, pod ktorou je spustený D2000 Server. Napríklad ak je použitá skupina *d2users*, tak treba spusti:
  chgrp d2users /etc/krb5.keytab
  chmod 640 /etc/krb5.keytab

Na platforme Linux bola otestovaná autentifkácia v rámci jednej domény (*IPSTEST.SK*) aj medzi dvoma doménami (hi.exe spustené pod užívateom v doméne *IPESOFT.SK*, D2000 server na Linuxovom serveri v doméne *IPSTEST.SK*. V oboch prípadoch bola hodnota parametra AuthSecPrinc nastavená na *SRVAPP$@IPSTEST.SK*, kde *SRVAPP* je názov linuxového poítaa zaradeného vo Windows doméne.

Metódy autentifikácie

V systéme D2000 sú podporované nasledovné metódy autentifikácie:

Metóda autentifikácie	Popis
D2000	Overovanie užívateského mena a hesla procesom D2000 Server. Toto je štandardná metóda autentifikácie, ktorá využíva meno a heslo uložené v konfigurácii objektu Užívate. Prihlasovací dialóg zobrazuje užívateské meno a heslo: 

NTLM	Overovanie mena a hesla zadaného užívateom vykonáva autentifikaný subsystém Windows NTLM (NT LAN Manager) dostupný od verzie Windows NT 4.0, priom sa autentifikácia vykonáva v doméne, ktorú udáva konfiguraný parameter užívatea Doména. D2000 Server získa po dokonení autentifikácie od Windows informáciu o úspešnom/neúspešnom overení užívateského mena a hesla v doméne. Pokia bola autentifikácia úspešná, poda užívateského mena vyhadá objekt typu Užívate a skontroluje, i má užívate nakonfigurovanú autentifikanú metódu NTLM ako povolenú (parameter Metódy autentifikácie), i je zhodný názov domény a i nemá za kázané prihlásenie. Prihlasovací dialóg zobrazuje užívateské meno a heslo, v záhlaví má okrem názvu aplikácie aj text *[NTLM]* a pod menom a heslom doménu, do ktorej sa užívate prihlasuje:  **Poznámka:** NTLM autentifikácia je použitená na samostatnom poítai s lokálne definovanými užívatemi (vtedy Doména je názov poítaa) ako aj vo Windows doméne (Doména je názov domény). Ak nie je možné kontaktova autentifikanú autoritu, prihlásenie neprebehne. Prihlasovanie sa zmení na autentifikáciu poda D2000 a užívateovi sa zobrazí upozornenie "Neúspešná NTLM autentifikácia. Zadajte prihlasovacie meno a heslo z D2000."
Kerberos	Overovanie identity užívatea vykonáva autentifikaný subsystém Windows Kerberos dostupný od verzie Windows 2000. Overuje sa identita užívatea prihláseného do Windows, takže prihlasovanie je automatické bez prihlasovacieho okna a bez zadávania mena a hesla. D2000 Server získa od Windows Kerberos autentifikaného subsystému informáciu o mene užívatea a doméne, v ktorej je prihlásený. Pokia názov domény zodpovedá konfiguranému parametru Doména, poda užívateského mena vyhadá objekt typu Užívate a skontroluje, i má užívate nakonfigurovanú autentifikanú metódu Kerberos ako povolenú (parameter Metódy autentifikácie) a i nemá za kázané prihlásenie. **Poznámka:** Sama o sebe je autentifikaná metóda Kerberos skoro tak nebezpená, ako nakonfigurovanie parametrov /AN a /AP, ktoré umožní spustenie procesu HI bez zadania mena a hesla, pokia užívate odíde od poítaa bez zamknutia pracovnej plochy (zadanie štartovacích parametrov je ešte o nieo menej bezpené, pretože je z nich možné heslo spätne vyíta, priom autentifikácia Kerberos umožuje iba okamžité zneužitie, ale nie zistenie hesla). Preto odporúame: • pouenie užívateov, aby pred odchodom od poítaa vždy zamkli pracovnú plochu alebo sa odhlásili, • povolenie Kerberos autentifikácie v zabezpeených priestoroch, kde nehrozí zneužitie, • používanie hardvérových kúov na prihlasovanie užívateov do Windows (USB token, security card a iné), ktoré po vytiahnutí automaticky zamknú pracovnú plochu. **Poznámka:** Kerberos autentifikácia je použitená iba vo Windows doméne, nie na samostatnom poítai, pretože vyžaduje softvérovú infraštruktúru, ktorá sa inštaluje iba ako súas radia domény Windows.
SPNEGO	Metóda autentifikácie dostupná až vo verziách novších ako D2000 12.00.061. Overovanie identity webového užívatea (Tenký klient a Smart Web) vykonáva autentifikaný subsystém Windows Kerberos dostupný od verzie Windows 2000. Overuje sa identita užívatea prihláseného do Windows, takže prihlasovanie je v prehliadai automatické bez prihlasovacieho okna a bez zadávania mena a hesla. D2000 Server získa od Windows Kerberos autentifikaného subsystému informáciu o mene užívatea a doméne, v ktorej je prihlásený. Pokia názov domény zodpovedá konfiguranému parametru Doména, poda užívateského mena vyhadá objekt typu Užívate a skontroluje, i má užívate nakonfigurovanú autentifikanú metódu SPNEGO ako povolenú (parameter Metódy autentifikácie) a i nemá z akázané prihlásenie. **Poznámka:** SPNEGO autentifikácia je použitená iba vo Windows doméne, nie na samostatnom poítai, pretože vyžaduje softvérovú infraštruktúru, ktorá sa inštaluje iba ako súas radia domény Windows.
RFID	Metóda autentifikácie dostupná od D2000 verzie 9.1.30. Užívate sa identifikuje zosnímaním RFID karty. Pre funknos RFID autentifikácie musí by RFID sníma nainštalovaný na klientskom poítai v niektorom zo sériových COM portov, musí beža proces D2000 HI s parametrami (parametre konzoly), ktoré zabezpeia, aby dokázal sníma obsluhova. Vi Nastavenia konzoly - RFID parametre. Po zosnímaní RFID karty môžu nasta dva prípady: 1. V D2000 HI nie je otvorená žiadna schéma, ktorá implementuje <ENTRY OnRFID> - vtedy HI automaticky prihlási užívatea s danou RFID kartou. 2. V D2000 HI je otvorená aspo jedna schéma, ktorá implementuje <ENTRY OnRFID> - vtedy HI neprihlási užívatea, ale zavolá udalos OnRFID do všetkých schém, ktoré túto udalos implementujú a ponechá obsluhu udalosti na aplikaný skript.

Poznámka 1: Pre iné operané systémy ako Windows je podporovaná iba autentifikácia D2000.
Poznámka 2: Pre iné metódy autentifikácie ako D2000 je potrebná dynamická knižnica d2auth.dll (nachádza sa v adresári D2000.EXE\bin).
Poznámka 3: Iné metódy autentifikácie ako D2000 sú podporené pre nasledovné procesy a moduly D2000: D2000 HI, D2000 GrEditor, D2000 CNF, D2000 Management Console, D2000 DDE Server, D2000 System Console, D2000 Tell, D2000 Browser, D2000 ODBC Driver.

Konfigurané parametre autentifikácie

Na konfiguráciu metód a parametrov autentifikácie slúžia nasledovné konfigurané parametre autentifikácie:

Názov parametra	Popis
AuthMethod	Prednastavená metóda autentifikácie, ktorú vyžaduje proces D2000 Server od všetkých prihlasujúcich sa užívateov. Možné hodnoty parametra sú: • D2000 • NTLM • Kerberos • SPNEGO (Iba pre Tenký klient a SmartWeb)
AuthSecPrinc	Security principal autentifikácie. Parameter je vyžadovaný v Kerberos a SPNEGO autentifikácii. Security principal môže by názov útu, pod ktorým je spustený proces D2000 Server. Štandardne (kernel.exe je spustený ako servis pod útom *Local System*) je *Security principal* úet poítaa v doméne, ktorého názov je rovnaký ako názov poítaa a na konci má znak dolár ($). Pokia je proces kernel.exe spustený rune (z príkazového riadku), je *Security principal* úet príslušného užívatea v doméne. **Príklad:** Doména je MyCompany, server je SrvApp1, proces kernel.exe je spustený ako servis pod útom *Local System*. Parameter AuthSecPrinc môže by *srvapp1$* alebo *srvapp1$@MyCompany* . Pokia sa chcú autentifikova aj užívatelia z inej domény OtherCompany, musí by AuthSecPrinc=*srvapp1$@MyCompany* a navyše doména MyCompany musí dôverova doméne OtherCompany. **Poznámka:** autentifikácia medzi doménami bola vyskúšané na serveri srvapp114v v doméne ipstest.sk, AuthSecPrinc=*srvapp114v$@ipstest.sk*. HI bolo spustené na poítai v doméne IPESOFT, doména ipstest.sk dôverovala doméne IPESOFT. **Príklad:** Doména je MyCompany, proces kernel.exe je spustený z príkazového riadka užívateom D2User. Parameter AuthSecPrinc môže by *d2user* alebo *d2user@MyCompany.* **Poznámka:** Pomocou nástrojov na správu Active Directory je možné definova aj Security principal, ktorý nie je závislý od mena užívatea, pod ktorým je proces kernel.exe spustený. Viac informácií vi dokumentácia k Active Directory a k utilite ktpass.exe na webe Microsoftu.

Paralelné použitie viacerých autentifikaných metód

Pri autentifikácii NTLM/Kerberos sa užívateské meno ani heslo neprenáša medzi poítaom s procesom D2000 Server a poítaom, kde beží užívateský proces (HI, Cnf, GrEditor at). Miesto toho sa po sieti prenášajú iba tzv. tokeny, ktoré si vymieajú autentifikané subsystémy Windows NTLM/Kerberos medzi týmito poítami a radiom domény. Preto autentifikácia NTLM/Kerberos nebude fungova, pokia je doménový radi (domain controller) nedostupný (porucha /vypnutie doménového radia, prístup klienta spoza firewallu at).

Z týchto dôvodov, ako aj z dôvodov konfiguranej flexibility, môže klientsky proces (HI, Cnf, GrEditor at.) použi inú metódu autentifikácie, ako je štandardná nakonfigurovaná parametrom AuthMethod za predpokladov, že:

- pre zvolenú metódu sú správne nakonfigurované všetky konfigurané parametre (t.j. Doména pre NTLM/Kerberos a AuthSecPrinc pre Kerberos),
- užívate má povolenú zvolenú autentifikanú metódu vo svojich Metódach autentifikácie.

Výber inej metódy autentifikácie je možný pomocou štartovacieho parametra klientskeho procesu /AF<Method>, v prípade D2000 ODBC Driver sa metóda autentifikácie explicitne konfiguruje v konfigurácii DSN.

Poznámka: Proces D2000 Server pri každom prihlásení sa procesu, ktorý podporuje prihlasovanie užívatea (HI, Cnf, GrEditor at), naíta konfigurané parametre autentifikácie z Windows registry a pošle ich prihlasujúcemu sa procesu. Je to kvôli možnosti dynamicky zmeni prednastavenú metódu autentifikácie poas behu systému D2000 (napr. poas výpadku doménového radia) a umožni tak užívateom, aby reštartovali HI a prihlásili sa do aplikácie inou autentifikanou metódou (D2000) bez potreby upravovania štartovacích parametrov HI konzol všetkých užívateov. Samozrejme takýto scenár vyžaduje, aby každý užívate mal povolenú autentifikanú metódu D2000 a navyše poznal svoje "záložné" heslo do D2000 uložené v konfigurácii užívatea.

Debugovanie autentifikácie

Na debugovanie autentifikácie slúži kategória Debug informácií **DBG.Authentication**, ktorá sa dá zapnú pri štarte procesu štartovacím parametrom **/E+DBG.Authentication** alebo poas behu procesu pomocou D2000 System Console.
Po zapnutí debugovania bude log procesu D2000 Server alebo log klientskeho procesu (HI, Cnf, GrEditor at.) obsahova podrobné výpisy o jednotlivých fázach autentifikácie (pre NTLM a Kerberos autentifikáciu), ktoré sú použitené pre úely technickej podpory.

Súvisiace stránky:

Konfigurácia aplikácie