Uživatelská příručka k pGině

http://pgina.xpasystems.com

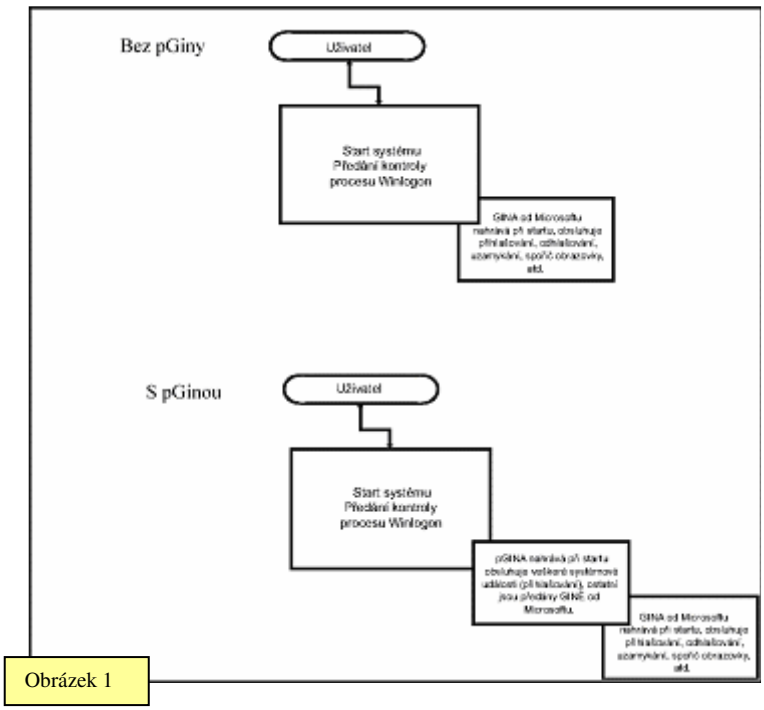
http://www.xpasystems.com

Překlad: Miroslav Dvořák (Miroslav.Dvorak@vsb.cz)

Předmluva

pGina je, ve zkratce, náhrada pro doménové přihlašování v prostředí Windows. pGina díky své technologii zásuvných modulů umožňuje správci výběr z mnoha existujících autentikačních zdrojů a metod. Dovoluje také správci realizovat jeho vlastní autentikační metodu nebo mu umožní rozšířit metodu existující. Správce může také snadno vytvořit svůj vlastní zásuvný modul podle přiloženého příkladu a pomocí API zásuvných modulů.

pGina pracuje tak, že se vloží do operačního systému Windows jako modul GINA (Graphical Identification and Authentication) – odtud to jméno. Pokud není pGina nainstalována, tak když začnou Windows startovat je volán proces Winlogon, který nahraje Microsoft GINA, která zachytává systémové události, jako je CTRL+ALT+DEL, aktivace spořiče obrazovky, pokus o přihlášení, atd. Pokud je pGina nainstalována, vloží se mezi proces Winlogon a GINU od Microsoftu a zachytává všechny tyto události sama a volá své vlastní události (přihlašování, uzamykání obrazovky, atd.). Všechny ostatní události předává transparentně modulu od Microsoftu.



Obrázek 1

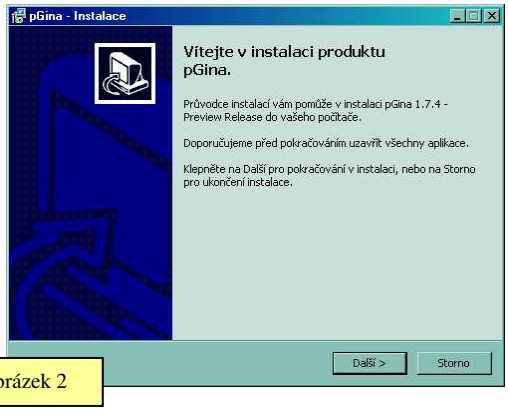
Pokaždé, když je pGina nahrána procesem Winlogon, pokusí se zavést zásuvný modul zvolený správcem. Když se pokusí uživatel přihlásit, pGina použije zvolený zásuvný modul k rozpoznání, zda uživatel může být autentikován, či nikoliv. Pokud zásuvný modul určí, že uživatel může pokračovat s přihlášením, pGina mu vytvoří lokální účet, přidá ho do skupin v zásuvném modulu specifikovaných, připojí disky jak nastavené globálně, tak disky specifické přímo pro uživatele, a mnoho dalších věcí zvolených v konfiguraci.

K pochopení, jak může pGina pomoci, mějme správce běžného nazvaného Franta. Franta je zodpovědný za mnoho počítačů s Windows 2000, stejně jako za mnoho počítačů s Linuxem. V současné době musí Franta udržovat duplicitní jména a hesla na serveru pro Windows a na UNIXovém serveru. Ještě k tomu je UNIXový server centrální souborový server. Všechno co dělá Windows server je, že autentikuje uživatele. Všichni jeho Linuxoví klienti se autentikují pomocí LDAPu. Franta tedy může použít pGinu k autentikování všech windowsových uživatelů ze stejného UNIXového serveru jednoduše tak, že ji nainstaluje a pak nainstaluje zásuvný modul pro LDAP. Nyní Franta spravuje pouze jediný zdroj s hesly a uživatelskými jmény a dále už nepotřebuje windowsový server. To mu uvolní mnoho času k vyřešení jiných úkolů a zredukuje mu to režie s maximálním počtem uživatelů na windowsovém serveru.

Instalace

Instalace pGiny je ověřená a dodržuje zvyklosti, které dodržují i jiné Windowsové programy. ***Důležitá poznámka: pGina může kdykoliv havarovat, stát se nepoužitelnou. To má za následek znepřístupnění systému. Z takových důvodů je důležité vědět, jak nastartovat do Stavu nouze, mít záchrannou disketu, nebo vědět, jak vzdáleně editovat registry.***

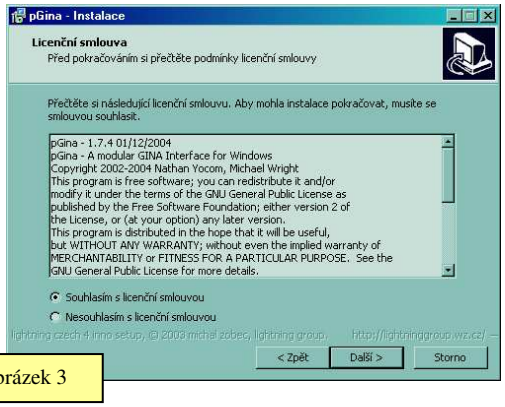
Takže od začátku: musíte stáhnout nejnovější verzi instalátoru ze stránky http://pgina.xpasystems.com. Poté si ověřte, zda jste přihlášen jako lokální správce (nebo máte práva lokálního správce), že váš počítač NENÍ členem domény (ledaže byste použil zásuvný modul, který spolupracuje s doménou) a spusťte instalátor. Potvrďte, že chcete pGinu instalovat a ukáže se vám obrazovka podobná obrázku 2.



Obrázek 2

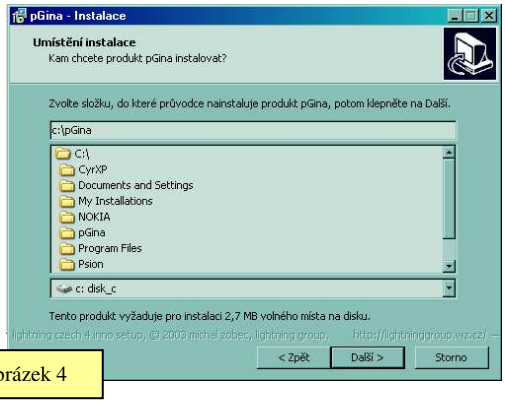
Po spuštění instalačního programu a výběru jazyka instalace vás přivítá instalátor pGiny.

Následující text vás provede standardní instalací pGiny. Stiskem tlačítka Další pokračujte k obrázku 3.



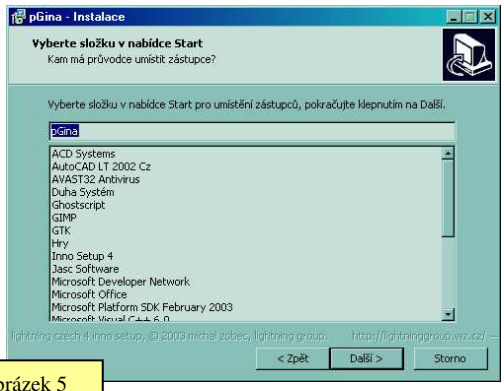
Obrázek 3

Tento dialog zobrazuje kopii GNU/GPL licence. Pokud jste si jistí, že rozumíte a souhlasíte zvolte "Souhlasím s licenčními podmínkami" a stiskněte tlačítko "Další". Tím pokročíte k obrázku 4.



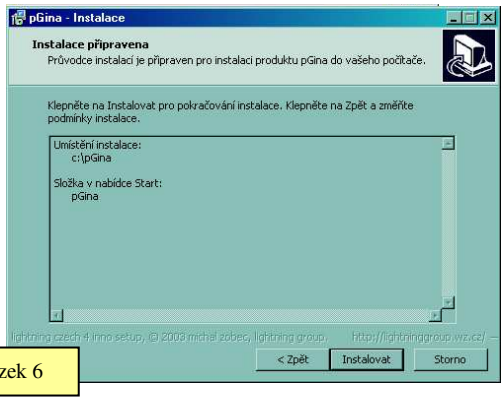
Obrázek 4

Nyní budete vyzváni k zadání cesty, kam nainstalovat pGinu a potřebné soubory. Zvolte jinou složku nebo pokračujte tlačítkem "Další" na obrázek 5.



Obrázek 5

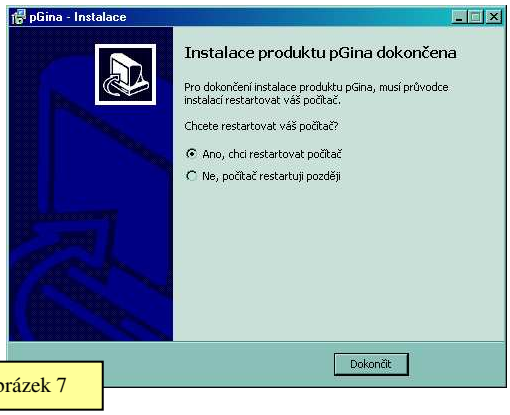
Nyní můžete zvolit, ve které složce v uživatelském menu pGina vytvoří svůj odkaz. Po zvolení pokračujte tlačítkem "Další" na obrázek 6.



Obrázek 6

Tato obrazovka vám dovolí zkontrolovat vaše dřívější volby. Ke změně těchto voleb použijte tlačítko "Zpět" a cokoliv změňte. Po zvolení "Instalovat" budou všechny nezbytné soubory rozbaleny a nainstalovány na váš systém do zvolených složek.

Jak je pravidlem, standardní instalace bude fungovat na většině systémů, avšak je doporučeno nerestartovat, dokud neověříte konfiguraci pGiny. Obrázek 7 ukazuje závěrečné dialogové okno instalační procedury.



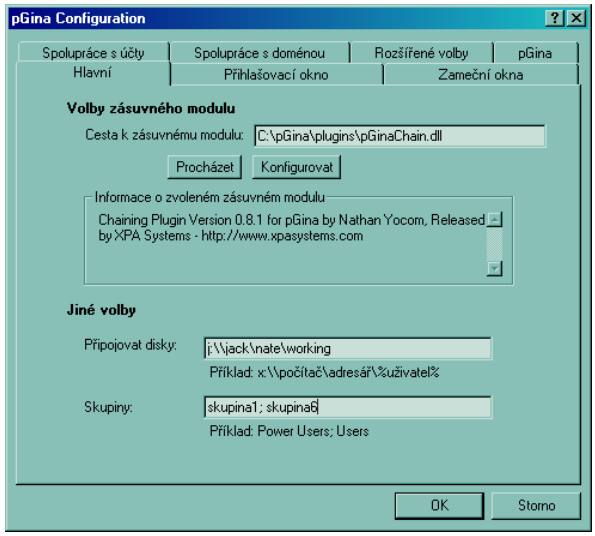
Obrázek 7

Pokud chcete restartovat počítač po dokončení instalace, zvolte „Ano, chci restartovat počítač", pokud ne, zvolte „Ne, počítač restartuji později".

Konfigurace pGiny

Pokud chcete konfigurovat pGinu, přihlaste se jako Administrátor, nebo mějte administrátorská oprávnění. Spusťte Konfigurační nástroj pGiny Start->Programy->pGina->Configuration Tool. Poté, co se krátce zobrazí úvodní obrazovka bude spuštěna hlavní konfigurační obrazovka. Těmito dialogy můžete měnit nastavení a veškeré volby pGiny. Pojďme si ukázat všechna jednotlivá nastavení a jejich působení na pGinu.

KONFIGURACE HLAVNÍ



Nejvíce používaná nastavení jsou v záložce Hlavní. To obsahuje zvolený zásuvný modul, který bude pGina využívat pro autentikaci, disky, které se budou mapovat každému uživateli a konečně skupinu, která bude každému uživateli přiřazena.

Volby zásuvného modulu
K výběru a nebo změně zásuvného modulu klikněte na tlačítko Procházet a zvolte soubor se zásuvným modulem. Informace o zvoleném zásuvném modulu budou zobrazeny v dialogu „Informace o zásuvném modulu“. Pokud zásuvný modul dovoluje individuální konfiguraci, kliknutím na tlačítko Konfigurovat ze zobrazí okno s konfiguračními parametry zásuvného modulu.

Jiné volby
Na panelu Hlavní je také volba Připojovat disky. Pokud je zvolena, všechny vepsané disky se připojí všem uživatelům, kteří se úspěšně přihlásí. Disky jsou specifikovány jako DISK:\\CESTA-KE-SDÍLENÍ, např.: přimapovat disk J z \\jack\nate\working musíte zvolit J:\\jack\nate\working. Více disků může být zadáno také, musí ale být odděleny středníkem.

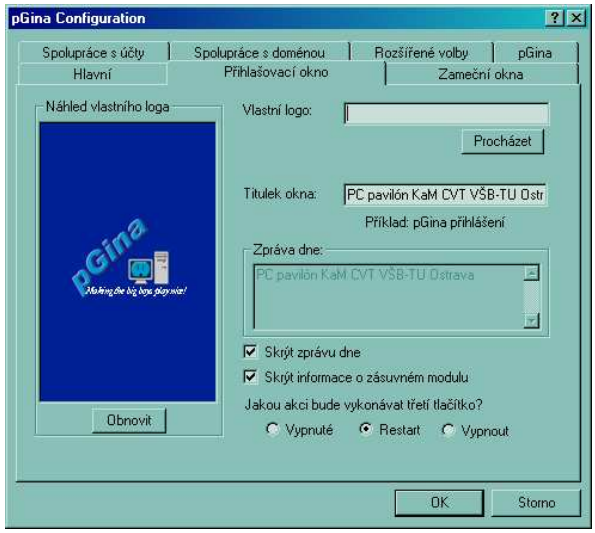
Dále můžete specifikovat, do kterých skupin budou všichni uživatelé zařazeni. Výčet skupin musí být opět oddělen středníkem, např.: pokud mají být všichni uživatelé ve skupině Users, ale také ve skupině Power Users, zadáte „Users;Power Users” bez uvozovek.

Volby v záložce „Rozšířené volby” z předchozích verzí přesunuty do vlastní záložky “Profily”.

„Ukázat výběr autentikační metody” – tato experimentální volba přidává možnost výběrového okna do přihlašovacího dialogu, který dovoluje uživateli výběr autentikace podle lokální stanice, domény nebo pomocí zásuvného modulu. Pokud zvolená možnost selže, selže také autentikace (na rozdíl od standardního nastavení pGiny, kdy se zkouší všechny metody v pořadí zásuvný modul, doména, lokální přihlašovací údaje).

„Jméno k zobrazení na výběru“ – pokud je zatržena volba „Ukázat výběr autentikační metody“, v seznamu pro výběr se ukáže tento název místo názvu zásuvného modulu. Tato volba umožňuje správci vložit údaje jako „LDAP server univerzity“ nebo jiné informace pro uživatele, co ten konkrétní zásuvný modul dělá.

KOFIGURACE PŘIHLAŠOVACÍ OKNO



Kliknutím na záložku Přihlašovací okno získáte přístup ke všem volbám, které mají vliv na vzhled a chování přihlašovacího okna.

Můžete použít tlačítko Procházet k výběru bitmapového obrázku, který bude použit v přihlašovacím okně jako logo. Jakmile je obrázek zvolen a je platný, bude zobrazen vlevo v okně Náhled vlastního loga (pokud ne, můžete použít tlačítko Obnovit k aktualizování náhledu). Tento dialog zobrazuje logo tak jak je zobrazeno při přihlašovacím dialogu. Standardní logo, které obsahuje pGina je 100 bodů široké a 146 bodů vysoké a má rozlišení 300x300 při barevné hloubce 24 bitů. Platné jsou pouze bitmapové obrázky.

Volba Titulek okna vám umožní zadat titulek pro přihlašovací okno.

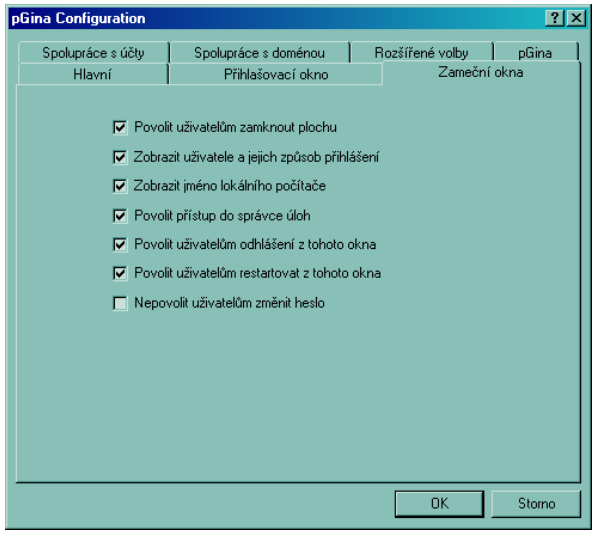
Zpráva dne je zobrazována nad dialogovými okny pro jméno a heslo na přihlašovacím okně. Jak je zvykem, text %machine% je nahrazen za běhu názvem lokálního počítače (bez přípony DNS). Pokud zvolíte Skrýt zprávu dne, nebudete moci text měnit (a samozřejmě nebude nikdy zobrazen).

Informace o zásuvném modulu (ty, které jsou zobrazeny v záložce Hlavní) jsou zobrazovány pod dialogovými okny pro jména a heslo. Pokud chcete raději tyto informace nezobrazovat, stačí kliknout na Skrýt informace o zásuvném modulu.

Třetí tlačítko, které je na přihlašovacím okně je konfigurovatelné. Toto tlačítko může být Vypnuté, může Restartovat a nebo Vypnout počítač.

Nyní můžete použít makro %ip% v textu zprávy. Při prvním spuštění to však může ukázat ip adresu 0.0.0.0, protože síť ještě nebyla nastavena

KONFIGURACE ZAMČENÍ OKNA



Toto okno je zobrazeno, pokud uživatel použije CTRL+ALT+DEL, když je přihlášen. Okno je také konfigurovatelné.

Jestliže **není** zatržena volba "Povolit uživatelům zamknout plochu" volba vypne tlačítko Zamknout.

Jestliže je zatržena druhá volba, uživatelské jméno a způsob jeho přihlášení (Zásuvným modulem, Doménovým přihlášením) je zobrazován.

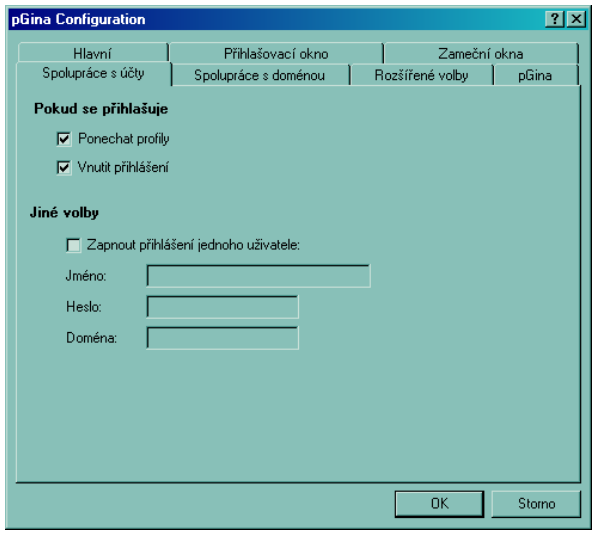
Jestliže je třetí zatržena, bude zobrazeno jméno lokálního počítače.

Jestliže **není** zatržena čtvrtá, volba Správce úloh bude vypnutá (Toto však nevypíná možnost použít klávesové zkratky jako je třeba CTRL+SHIFT+ESC).

Poslední dvě mají vliv na to, aby uživatel měl možnost zamknout plochu či restartovat.

"Nepovolit uživatelům změnit heslo" znemožní uživateli změnit heslo při stisku Crtl+Alt+Del. "Povolit administrátorovi odemknout plochu uživatele" povolí „skutečné odemknutí", což znamená, že administrátor může odemknout plochu uživatele, *aniž by ho při tom odhlásil*. Volba Vlastní logo nastaví logo na zamknuté obrazovce.

SPOLUPRÁCE S ÚČTY



Při úspěšném autentikování skrze zásuvný modul pGina vytvoří lokální účet se jménem, kterým se uživatel přihlásil. To znamená, že se na disku vytvoří profil (odpovídající nastavení politiky na počítači a nastavení Defaultního profilu ve Windows samotných). Správa tohoto chování je možná na záložce Spolupráce s účty.

Pokud je zatržena volba Ponechat profily, účet na disku a profil **nejsou** po odhlášení smazány. To znamená, že profily jsou mezi dvěmi přihlášeními uchovány. Pokud **není** zatrženo, profily a lokální účty jsou vymazány z počítače. V konečném důsledku to znamená, že při každém novém přihlášení se vytvoří nový účet založený na standardním nastavení počítače a Windows.

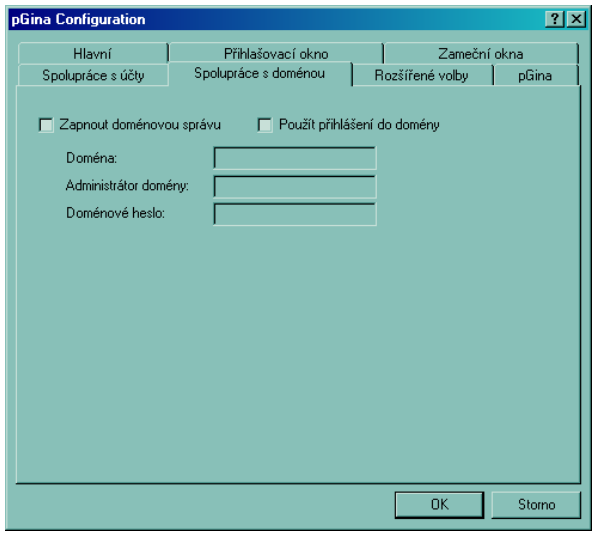
Kdykoliv, pokud je volba Ponechat profily aktivní, je možné, že uživatelské heslo se může kdekoliv změnit. Výsledkem toho bude, že uživatel bude autentikován zásuvným modulem, avšak heslo na lokálním profilu může být jiné. Pokud je zatržena volba Vnutit přihlášení je tato nepříjemnost eliminována vnucením lokálního hesla tak, aby souhlasilo s heslem autentikovaným zásuvným modulem při přihlášení.

Dostupná je také volba Zapnout přihlášení jednoho uživatele. Pokud je tato použita, zadané heslo a jméno (a doména, pokud je zadána, jinak se předpokládá lokální účet) se použijí pro přihlášení uživatele daným jménem a heslem (a doménou, pokud je zadána, jinak se přepokládá lokální účet), místo jména a hesla autentikovaného zásuvným modulem. Toto dovoluje filtrovat přístup na jeden účet autentikovaný jiným účtem, tj. autentikovaný zásuvným modulem a přihlášený jiným uživatelem zadaným v této položce. Pokud je tato volba použita, volby Ponechat profily a Vnutit přihlášení nemají žádný efekt.

Pokud je zatržena volba "Ponechat uzamčené účty" spolu s „Vnutit přihlášení", pGina NEZMĚNÍ nastavení a heslo uzamčeného/zakázaného účtu, pokud ho přihlásí.

Volba „Povolit ukládání účtů a vypršení" bude vytvářet lokální účet s přednastavenou dobou platnosti a bude použit v návaznosti na přihlášení do domény. Čas vypršení je v sekundách. Toto je EXPERIMENTÁLNÍ vlastnost a měla by být použita, **pouze pokud jste si jisti**, že ji potřebujete.

SPOLUPRÁCE S DOMÉNOU

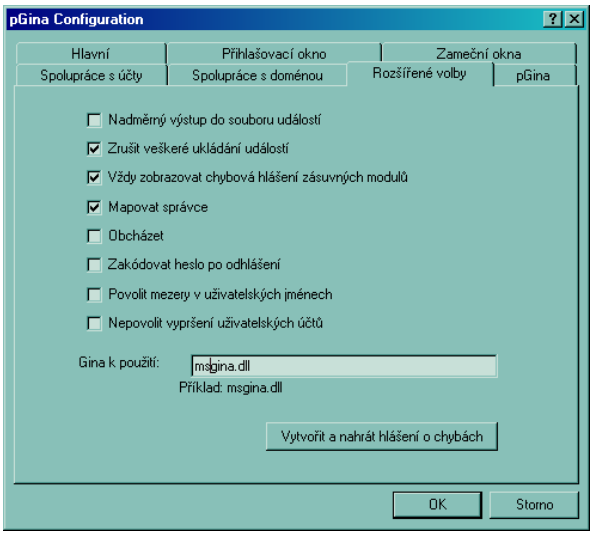


pGina má také několik voleb, které dokáží úzce spolupracovat s existující doménovou infrastrukturou. I když to nebyl původní záměr pGiny, ukázalo se, že v některých instalacích je to velice užitečné a potřebné. Pokud je zatržena volba „Použít přihlášení do domény", daná doména bude také použita v autentikačním procesu. Proces probíhá tak, že pGina nejprve použije zásuvný modul, posléze přihlašování do domény a nakonec autentikaci na lokálním počítači.

Zapnout doménovou správu je volba, při které pGina přesměrovává svojí správu účtů (viz. odstavec Spolupráce s účty) na uvedenou doménu. To znamená, že účty budou tvořeny, mazány a spravovány tak, jak to umí pGina dělat na lokálním počítači. pGina 1.7.4 k tomu potřebuje buď NT4 server nebo nějaký Active Directory Server spuštěný v Mixed Modu (podpora čistého AD je plánována v budoucích verzích). Samozřejmě pGina musí znát administrátorské jméno a heslo, aby mohla dělat všechny potřebné změny.

ROZŠÍŘENÉ VOLBY

Poslední konfigurační záložka jsou Rozšířené volby.



Zvolením Nadměrný výstup do souboru událostí zajistíte to, že pGina bude vytvářet ladicí log v souboru událostí, který je dostupný administrátorskými nástroji.

Pokud je však zvolena volba Zrušit veškeré ukládání událostí, nebudou události jak ladicí, tak i obyčejné do systémových souborů ukládány.

Pokud je zatrženo Vždy zobrazovat chybová hlášení zásuvných modulů, bude zobrazen chybový výstup zásuvného modulu vždy, když se nepodaří uživatele autentikovat. Pokud není volba zatržena, zobrazí se chyba pouze, pokud totálně selže přihlašování.

V základním nastavení pGina používá Mapovat disky z Hlavní konfigurace pouze pro uživatele, kteří byli autentikování zvoleným zásuvným modulem. Pokud je však zvolena volba Mapovat správce, administrátorským účtům jsou také připojeny zvolené disky.

Pokud je zvoleno obcházet, pGina se „ukryje“ a postoupí všechnu kontrolu standardní Gině od Microsoftu. Výsledkem je standardní chování přihlašování do Windows.

Občas je nutné, aby pGina ponechávala uživatelské profily na disku (možno změnit v záložce Spolupráce s účty). Nicméně profily zanechané na disku obsahují i heslo, které bylo platné v době přihlášení. Pokud je pak ztraceno připojení k síti nebo selže autentikace pomocí zásuvného modulu a lokální jméno a heslo souhlasí, je povoleno přihlášení. Volba Zakódovat heslo po odhlášení dovolí přepsání hesla náhodnými znaky vždy po odhlášení. Je nadmíru **žádoucí**, aby tato volba byla zatržena **pouze** v případě, že je také zatržena volba Vnutit přihlášení na záložce Spolupráce s účty. Pokud by tato volba nebyla zatržena, mělo by to za následek nemožnost přihlášení se na lokální účet.

Některé protokoly, jako třeba LDAP automaticky ignorují mezery v uživatelských jménech, pokud **není** zatrženo Povolit mezery v uživatelských účtech, pGina neautentikuje uživatele, kteří zadají uživatelské jméno s mezerou.

“Povolit EXPERIMENÁLNÍ podporu pro TS/RDP” zapne speciální kód v pGině, který zapíná podporu pro přihlášení pomocí TS/RDP (bez nutnosti dvojitého přihlašování). Volba je označena jako experimentální, protože mnoho z funkcí TS/RDP (autologin, zrušení==odpojení atd) není ještě implementováno.

Volba „Respektovat automatické přihlášení z registrů“ říká pGině, zda má automaticky přihlásit uživatele specifikovaného v dobře známém automatickém přihlašování v registrech. Pokud je volba zatržena, informace v registru je platná, uživatel bude přihlášen. Jinak je tato informace ignorována.

Jiné odkazy

Stránka pomoci Microsoftu “Nastavování uživatelského prostředí Defaultního uživatele”:
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q305709

Další dokumentace k pGině
http://pgina.xpasystems.com

On-line diskusní fórum
http://forums.xpasystems.com/

Profesionální konzultace, implementace a podpora
http://www.xpasystems.com

E-mailové konference
Hlavní: http://lists.sourceforge.net/mailman/listinfo/pgina-general
Aktualizace: http://lists.sourceforge.net/mailman/listinfo/pgina-updates
Vývojáři: http://lists.sourceforge.net/mailman/listinfo/pgina-devel

Jiná dokumentace k GINA
http://msdn.microsoft.com/library/en-us/security/security/winlogon_and_gina_start_page.asp