

IX Seminarium PLOUG
Warszawa
Maj 2004

Integracja Oracle z domeną i Active Directory

Paweł Goleń, Stanisław Kipiel

Często spotkać można się z przeświadczeniem, że jeżeli tworzony jest poważny system, to baza danych na pewno nie zostanie zainstalowana na platformie Windows. Jeśli nawet uznać zasadność tej tezy, można zastanawiać się co w takim razie z systemami “mniej” poważnymi? Nie można również nie zauważać, że środowisko Windows jest powszechnie używane w wielu miejscach i raczej nic nie wskazuje, by sytuacja ta miała ulec gwałtownej zmianie. Oracle, choć zwykle z pewnym opóźnieniem, udostępnia swoje produkty również dla platformy firmy Microsoft, co więcej wzbogaca je o dodatkową funkcjonalność, która pozwala w pełni wykorzystać jej potencjał. Co ciekawego oferować może środowisko oparte o systemy Windows? Często system ten nie kojarzy się zbyt dobrze, zarówno jeśli chodzi o jego stabilność, jak i bezpieczeństwo. Po przełamaniu tradycyjnej niechęci związanej z produktami Microsoftu, okazuje się, że systemy Windows 2000, Windows XP oraz Windows 2003 pozwalają na stworzenie bezpiecznej, centralnie zarządzanej i zintegrowanej ze sobą platformy. Bardzo użytecznymi cechami takiej platformy jest centralne zarządzanie użytkownikami, oraz zunifikowane mechanizmy uwierzytelniania użytkowników. Najlepiej środowisko to wykorzystują produkty firmy Microsoft, czemu trudno się dziwić. Coraz częściej jednak także inne firmy tworzące oprogramowanie dla tego systemu starają się wykorzystać dostępne w nim mechanizmy. Do firm tych zaliczyć można również Oracle. W prezentacji tej rozważone zostaną zagadnienia centralnego zarządzania użytkownikami, oraz integracja mechanizmów PKI zawartych w Oracle i Windows.

Zarządzanie użytkownikami

Tworzone systemy informatyczne stają się coraz większe, kolejną częstą ich cechą jest duże rozproszenie, również geograficzne. W takim środowisku kwestia zarządzania użytkownikami i ich uprawnieniami staje się często poważnym problemem. Jeden użytkownik korzystać musi nagle z wielu różnych kont w systemie i wielu różnych haseł. Jest to uciążliwe. Jeszcze bardziej uciążliwe jest zarządzanie tak “rozproszonym” systemem. Z tego też powodu wykorzystywane są mechanizmy centralnej administracji, na przykład wykorzystujące centralną usługę katalogową (LDAP), co z kolei wymusza replikację danych do odległych oddziałów. Choć Oracle posiada własną usługę katalogową, jej wykorzystanie w niektórych przypadkach daje dość iluzoryczne zyski. Takim szczególnym przypadkiem jest sytuacja, w której baza Oracle wykorzystywana jest w środowisku opartym na systemach Windows.

Microsoft właściwie od pierwszych wersji systemu NT wykorzystywał mechanizmy centralnej administracji. Ogromny postęp nastąpił wraz z pojawieniem się systemu Windows 2000. Dotychczasowe mechanizmy domeny NT zostały zastąpione przez Active Directory. Jest to centralne repozytorium informacji na temat użytkowników i całej domeny, można za jego pośrednictwem dokładnie kontrolować środowisko pracy każdego użytkownika i konfigurację każdego komputera. Na każdej maszynie dołączonej do domeny można wykorzystać informacje o kontaktach użytkowników i przypisać im określone uprawnienia dostępu do jej zasobów. W ten prosty sposób użytkownicy kontrolowani są centralnie i korzystają z tego samego konta logując się do swojej stacji roboczej, usług sieciowych, bazy danych. Active Directory udostępnia interfejs LDAP, dzięki czemu można integrować z nim aplikacje zewnętrzne. Skoro w danym środowisku istnieje już centralne repozytorium, tworzenie nowego nie ma większego sensu. Prowadziłoby to albo do konieczności zapewnienia synchronizacji między dwiema usługami katalogowymi, albo do pojawienia się różnych kont, z których korzystać ma ten sam użytkownik, a tego właśnie chce się uniknąć. Nowe wersje Oracle wykorzystują mechanizmy systemu Windows do uwierzytelnienia użytkowników bazy danych. Dzięki temu użytkownik, który już raz uwierzytelił się w systemie, nie musi ponownie podawać swoich danych (nazwy użytkownika i hasła), przy próbie dostępu do bazy danych. Co więcej wykorzystanie Active Directory pozwala na wykorzystanie centralnego zarządzania użytkownikami, oraz ich uprawnieniami (rolami).

Systemy Windows wykorzystują kilka protokołów uwierzytelniania. Dla Windows 2000 i nowszych podstawowym protokołem jest Kerberos. Starsze systemy wykorzystują również protokół NTLM (dwie możliwości NTLM i NTLMv2, który jest protokołem bezpieczniejszym). Najstar-

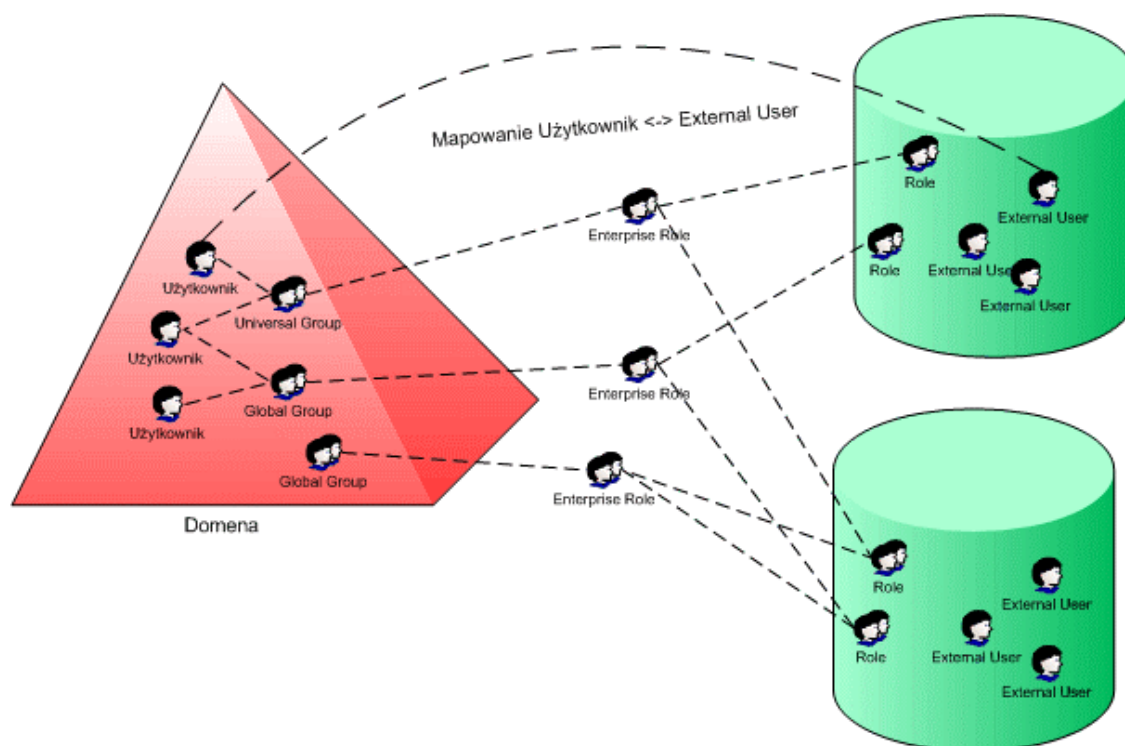
szym dostępnym protokołem jest LanManager, który jednak jest protokołem bardzo starym, stworzonym w czasach, gdy komputery miały jeszcze niewielką moc obliczeniową, a w efekcie protokół ten nie zapewnia praktycznie żadnego poziomu bezpieczeństwa. Dlaczego tak jest? W przypadku protokołu LM wykorzystywanych jest maksymalnie 14 znaków hasła (w przypadku, gdy hasło jest krótsze, jest uzupełniane do tej długości przez system). Hasło to dzielone jest na dwie niezależne od siebie części o długości 7 znaków, a dodatkowo wszystkie litery zamieniane są na duże. Z części tych generowany jest klucz wykorzystywany dalej do wyliczenia hasha. Postępowanie takie ogranicza efektywną długość hasła do 7 znaków, a przez brak rozróżnienia między dużymi a małymi literami dodatkowo zawęża przestrzeń, która musi być sprawdzona przy próbie złamania hasła. W przypadku NTLM sytuacja przedstawia się zdecydowanie lepiej. Wykorzystywane jest do 128 znaków hasła, wpisany ciąg zamieniany jest na unicode, a następnie jest z niego wyliczany skrót md4. Złamanie takiego hasha jest zdecydowanie trudniejsze niż w przypadku prymitywnego hasha LM. W przypadku Kerberosa poziom bezpieczeństwa może zostać dodatkowo polepszony poprzez wykorzystanie rozszerzeń PKI, dzięki czemu do uwierzytelnienia użytkownika w systemie wykorzystywany jest certyfikat, którego klucz prywatny jest bezpiecznie osadzony na karcie. Oracle potrafi wykorzystać protokoły NTLM oraz Kerberos. Do wykorzystania protokołu Kerberos konieczne jest jednak spełnienie dodatkowych wymagań (istnienie domeny, odpowiednie połączenie wersji produktów Oracle i wersji systemu Windows).

W normalnej sytuacji informacje o użytkownikach oraz ich uprawnieniach przechowywane są w bazie danych. W przypadku, gdy rośnie ilość użytkowników, oraz ilość wykorzystywanych baz, rozwiązanie takie staje się coraz bardziej niewygodne i nieefektywne. Pewnym rozwiązaniem tej sytuacji są tak zwani użytkownicy zewnętrzni. External users są zdefiniowani w zewnątrz, w stosunku do Oracle, repozytorium. W przypadku środowiska Windows definiowani są oni przez system operacyjny. W podstawowej formie użytkownicy zewnętrzni stosowani są zwykle w przypadku, gdy istnieje ich ograniczona liczba. Każdy użytkownik zewnętrzny musi zostać stworzony w każdej bazie danych, do której musi mieć dostęp. Podobnie jak użytkownicy, tak i zewnętrzne role muszą zostać zdefiniowane w każdej bazie oddzielnie. W przypadku, gdy wykorzystywany jest system Windows, Oracle wykorzystuje przynależność użytkowników do grup lokalnych w systemie. Zaletą tego rozwiązania jest brak konieczności posiadania serwera katalogowego. Jeśli jednak środowisko staje się zbyt duże, sprawa wygody zarządzania nim jest jednak co najmniej dyskusyjna. W przypadku, gdy tworzone środowisko zakłada wykorzystanie dużej ilości użytkowników i większej ilości baz danych (dodatkowo rozproszonych geograficznie) warto wykorzystać mechanizmy oferowane przez enterprise users oraz enterprise roles. Wymagają one jednak istnienia serwera katalogowego, w którym przechowywane będą informacje o użytkownikach i ich uprawnieniach. Standardowo jest do tego wykorzystywana usługa katalogowa dostarczana wraz z Oracle, jednakże do tego celu wykorzystane może być również Active Directory. Ważną cechą Active Directory jest jego przystosowanie do pracy w środowisku rozproszonym. Pojęcie "centralne repozytorium informacji" może być nieco mylące, gdyż w rzeczywistości usługa ta może być oferowana jednocześnie przez wiele różnych kontrolerów domeny. Dane zawarte w Active Directory replikowane są między poszczególnymi kontrolerami. Klienci korzystają z usług najbliższego dla nich kontrolera domeny, jeśli w ich lokacji nie ma działających kontrolerów, mogą skorzystać z maszyn bardziej odległych. Dzięki tym mechanizmom prawdopodobieństwo całkowitej awarii Active Directory jest dość znikome. To wszystko przemawia za potraktowaniem Active Directory jako wydajnego i bezpiecznego repozytorium danych, które wykorzystywane mogą być między innymi przez serwery baz danych Oracle.

Każdy z użytkowników enterprise users musi być zdefiniowany jako użytkownik zewnętrzny w każdej bazie, do której ma posiadać dostęp. Użytkowników takich mogą być tysiące, jednakże większość z nich nie będzie potrzebowała własnego schematu w bazie danych, ograniczyć można się do schematu aplikacji. Oracle pozwala na stworzenie jednej, dzielonej schemy, do której następnie można zmapować wielu enterprise users. Każdy enterprise user posiada przypisaną enterprise role. Jest to rola stworzona i przechowywana w usłudze katalogowej, do niej następnie przypisywane są role globalne i grupy stworzone w bazie danych, tak więc rolę tę przedstawić można

jako zbiór uprawnień w bazach danych. W domenie Windows każdy użytkownik należeć może do jednej lub wielu grup globalnych i uniwersalnych, do każdej z tych grup przypisać można enterprise roles.

Jak ostatecznie wygląda mapowanie uprawnień między Oracle i Active Directory? Użytkownicy istniejący w domenie posiadają obiekt, który reprezentuje każdego z nich w Active Directory. Obiekt ten posiada wszystkie cechy konieczne do wykorzystania go jako enterprise user w Oracle. Każdy użytkownik w domenie Windows przypisany może być do jednej lub wielu grup globalnych i uniwersalnych, a w bazie Oracle może zostać zdefiniowany natomiast jako external user. Do każdej grupy globalnej lub uniwersalnej przypisana może zostać enterprise role. Do każdej enterprise role przypisane mogą zostać role zdefiniowane w bazach danych. W efekcie użytkownicy istniejący w systemie Windows pojawiają się w bazie Oracle jako external users. Posiadają oni w niej uprawnienia wynikające z ich przynależności do grup zabezpieczeń, które poprzez enterprise roles mapowane są na role w bazie Oracle. W ten nieco może złożony sposób osiągany jest podobny stopień integracji, jaki zaoferować może baza MS SQL 2000, gdzie istnieje możliwość zdefiniowania w bazie danych użytkowników systemowych i przypisanie im określonych praw. Ogólny schemat powiązania Active Directory i Oracle przedstawiony jest poniżej.



Dodatkowo należy uwzględnić możliwość wykorzystania przez Oracle natywnych metod uwierzytelniania. Wszystko to powoduje zbliżenie Oracle i MS SQL 2000 pod względem łatwości zarządzania w infrastrukturze opartej o domenę Active Directory.

Dla lepszego zrozumienia tej zależności można posłużyć się następującym przykładem. Niech każdy użytkownik tworzony w Active Directory jest jednocześnie definiowany w bazach danych jako external user, a w systemie niech istnieją następujące role:

- pracownik_oddziału
- zarząd_oddziału
- zarząd_firmy

Role te nie ograniczają się w praktyce do samej bazy danych, użytkownicy tacy będą mieli prawdopodobnie dostęp do innych zasobów (dokumenty, pliki), który zależy również od ich roli w omawianej firmie. Można więc zakładać, że w Active Directory pojawią się grupy uniwersalne lub globalne odpowiadające rolom pracownik_oddziału, zarząd_oddziału, zarząd_firmy. Grupy te mapowane są na enterprise roles. Dzięki temu każdy z członków tych grup otrzymuje uprawnienia, które są niezbędne do wykonania jego pracy. W chwili, gdy pojawia się nowy pracownik, lub istniejący pracownik awansuje, cała zmiana uprawnień ogranicza się do przeniesienia lub dodania użytkownika do odpowiedniej grupy na poziomie domeny Active Directory, która to akcja skutkuje również przeniesieniem tego użytkownika do innej enterprise role, a co za tym idzie zmianą posiadanych przez użytkownika uprawnień. Nakład pracy na wyodrębnienie istniejących ról i stworzenie odpowiedniej hierarchii grup początkowo może być duży, późniejsza wygoda zarządzania jednak rekompensuje te problemy.

Aby osiągnąć takie możliwości konieczna jest oczywiście ingerencja w schemat Active Directory. Poszerzenie schemy jest konieczne do wykorzystania możliwości enterprise users oraz enterprise roles, jest to jednak realizowane automatycznie w trakcie instalacji Oracle.

PKI

W przypadku powiązania ze sobą mechanizmów PKI dostępnych w Oracle oraz w Windows należy rozważyć funkcjonowanie następujących elementów:

- Ze strony Oracle:
 - Oracle Wallet
 - Oracle Wallet Manager
 - Oracle Enterprise Login Assistant
- Ze strony Windows:
 - Microsoft Certificate Stores
 - Microsoft Certificate Services
 - Wallet Resource Locator

Certyfikat trzeba jakoś wystawić. Do tego celu wykorzystać można urząd certyfikacji, który wbudowany jest w system Windows. Jest on stosunkowo prosty w obsłudze i dobrze zintegrowany z Active Directory. Dzięki tej integracji możliwe jest między innymi automatyczne wystawianie określonych certyfikatów użytkownikom na podstawie informacji, które znajdują się w Active Directory. Oczywiście można urząd ten skonfigurować w taki sposób, aby działał w sposób mniej automatyczny, a większa kontrola przekazana była operatorom postępującym według określonych procedur.

Wystawione certyfikaty (wraz z kluczami prywatnymi) muszą być gdzieś przechowywane. O ile sam certyfikat nie jest newralgiczny, o tyle klucz prywatny powiązany z tym certyfikatem należy dobrze chronić. W tym celu zarówno Oracle jak i Microsoft opracował własne rozwiązania. W przypadku Oracle funkcjonalność ta jest realizowane przez Oracle Wallet, Microsoft wykorzystuje do tego Microsoft Certificate Stores. Zarówno Wallet jak i MCS przechowywać mogą certyfikaty, klucze, oraz tak zwane "trust points", czyli certyfikaty urzędów uznanych za zaufane. Certyfikaty wystawiane przez takie urzędy są uznawane za zaufane. Certyfikaty (i klucze) przechowywane zarówno w Oracle Wallet jak i MCS wykorzystywane mogą być do szyfrowania, podpisywania oraz uwierzytelnienia użytkownika. Która z metod przechowywania certyfikatów i kluczy jest bezpieczniejsza? Na to pytanie ciężko jest udzielić jednoznacznej odpowiedzi. Zarówno w MCS jak i Oracle Wallet przechowywane klucze są szyfrowane. O rozszyfrowanie, a następnie ponowne zaszyfrowanie zawartości Oracle Wallet dba Oracle Enterprise Login Assistant, w przypadku MCS obsługa przechowywania certyfikatów realizowana jest przez system operacyjny i jest powiązana z przechowywaniem profilu użytkownika. W obu przypadkach można uznać, że zarówno bezpieczeństwo kluczy jak i wygoda użytkownika jest zadowolająca. Z uwagi na zbliżoną

funkcjonalność naturalna jest chęć integracji ze sobą Oracle Wallet i MCS. Pozwoli ona również uniknąć problemów z przechowywaniem tego samego certyfikatu (i klucza) w dwóch różnych miejscach, o jakie problemy chodzi przekonać się może każdy użytkownik Mozilli, który obecnie przeszedł na Thunderbirda i Firefoxa. Wystarczy wspomnieć o tym, że w każdej z tych aplikacji należy niezależnie zarejestrować certyfikat zaufanego urzędu, certyfikaty serwerów, ludzi. Nie jest to zbyt wygodne, a czasami jest to po prostu irytujące. Oracle potrafi wykorzystać certyfikaty przechowywane w MCS, nie jest to specjalnie trudne, gdyż w systemie dostępne jest odpowiednie API. Do odnajdowania certyfikatów służy usługa Wallet Resource Locator, w przypadku, gdy wartość parametru WALLET_LOCATION zostanie ustawiona na MCS, Oracle Wallet wykorzystywać będzie certyfikaty zarejestrowane w magazynach użytkownika natywnych dla systemu Windows.