

Jak szybko możemy sprawdzić faktyczne uprawnienia użytkownika sieci? Ile czasu zajmuje wygenerowanie raportu zgodności z zasadami dostępu do udziałów? Czy można szybko sprawdzić, kto ostatni modyfikował wybrane pliki lub próbował uzyskać dostęp do zastrzeżonych zasobów? Do realizacji takich zadań służą systemy kontroli uprawnień.

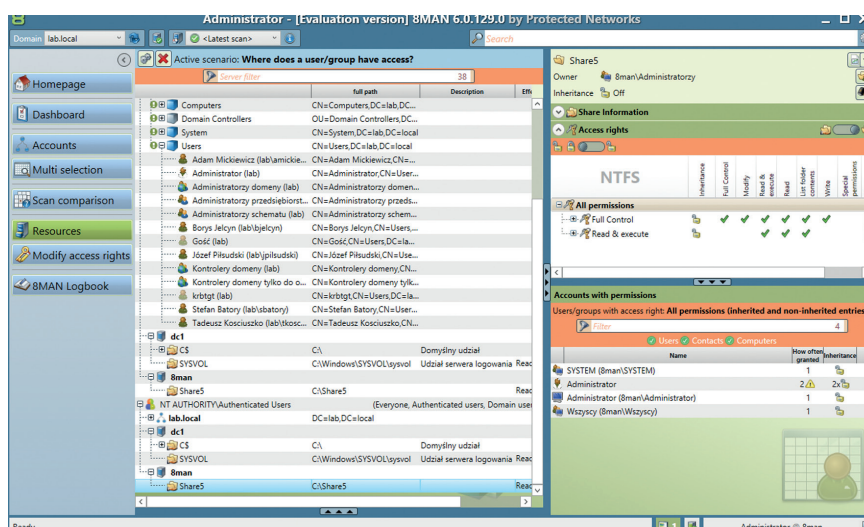
Kontrola uprawnień użytkowników

8MAN – Access Rights Management

Marcin Jurczyk

Jednym z najcenniejszych zasobów w otaczającym nas świecie jest informacja. O tym, jak istotna jest ochrona przechowywanych danych, świadczą chociażby nagłówki artykułów dotyczących afer będących skutkiem wycieku informacji. O ile zabezpieczenie przed infiltracją z zewnątrz i działaniem wykwalkowanych ekspertów w danej dziedzinie nie należy do trywialnych zadań, o tyle kontrola własnych zasobów i uprawnień przydzielanych poszczególnym użytkownikom powinna być traktowana jako absolutne minimum. Centralne zarządzanie oraz mechanizmy umożliwiające kontrolę nad użytkownikami zapewnia m.in. wykorzystanie usług katalogowych Active Directory i domen Windows.

Wraz z rozwojem organizacji panowanie nad uprawnieniami każdego użytkownika to coraz większe wyzwanie. W odpowiedzi na potrzeby administratorów powstał system 8MAN pozwalający na scentralizowane i zintegrowane zarządzanie uprawnieniami do wybranych zasobów informatycznych przedsiębiorstwa. 8MAN to produkt niemieckiej firmy Protected Networks z siedzibą w Berlinie, istniejącej na rynku rozwiązań do zarządzania uprawnieniami od 2009 roku. Oprogramowanie pozwala na kontrolę uprawnień użytkowników w środowiskach Microsoft Windows oraz VMware



Weryfikacja dostępu do zasobów dla poszczególnych użytkowników.

vSphere i udostępnia uproszczony, centralny interfejs zarządzania prawami dostępu dla serwerów plików, Exchange, SharePoint oraz vSphere.

> MOŻLIWOŚCI SYSTEMU

Narzędzie klasy Access Rights Management powinno umożliwiać łatwą kontrolę systemów autoryzacji z poziomu centralnego punktu zarządzania. 8MAN realizuje to założenie głównie dla środowiska opartego o rozwiązania Microsoftu. Za pośrednictwem graficznej konsoli administrator uzyskuje łatwy i szybki dostęp do systemu zarządzania uprawnieniami w przedsiębiorstwie, w którym wdrożono Active Directory.

Aplikacja została stworzona w technologii .NET, więc naturalnym środowiskiem jej pracy jest platforma Windows Server. Ścisła integracja z AD w połączeniu z intuicyjnym interfejsem graficznym 8MAN pozwala na pełny monitoring istniejącej struktury uprawnień w administrowanym środowisku IT. Wszelkie nieprawidłowości, takie jak zbyt rozległe uprawnienia niektórych użytkowników czy powielanie schematu uprawnień w ramach pojedynczej struktury organizacyjnej, można łatwo namierzyć i wyeliminować dzięki uproszczonej wizualizacji schematu uprawnień i wbudowanym raportom. Kontrolowane są uprawnienia AD i NTFS, odwzorowywana jest



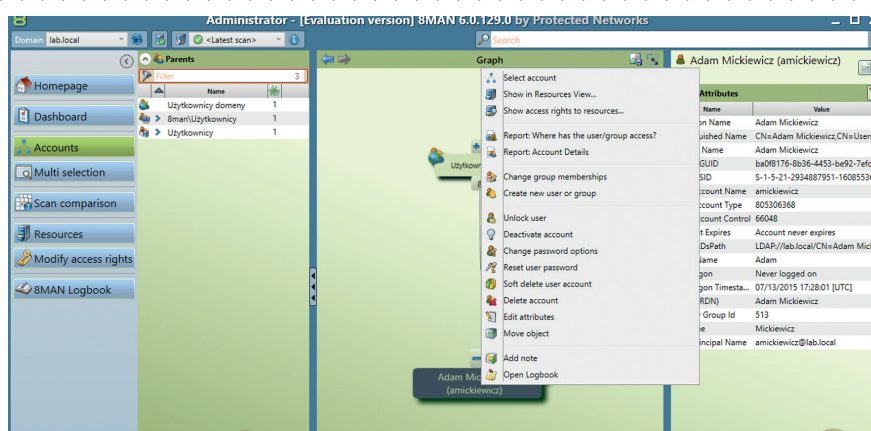
+ struktura organizacyjna przedsiębiorstwa i możliwe jest delegowanie zarządzania uprawnieniami do właścicieli poszczególnych zasobów.

W praktyce najbardziej przydatna okazuje się możliwość zarządzania uprawnieniami do usługi serwera plików. 8MAN współpracuje z rozwiązaniami EMC, Netapp oraz standardowymi rozwiązaniami serwera plików opartymi na CIFS. Dzięki takim opcjom testowanego systemu łatwo można sprawdzić kto, kiedy, jak długo i w jakim celu próbował uzyskać dostęp do współdzielonych zasobów. Ponadto 8MAN pozwala na administrowanie uprawnieniami bezpośrednio z wbudowanej konsoli zarządzania. Tworzenie nowych kont użytkownika AD i przydzielanie im odpowiednich uprawnień realizowane jest w sposób intuicyjny, z wykorzystaniem mechanizmów „przeciągnij i upuść”. 8MAN umożliwia również przydzielanie uprawnień tymczasowych w ściśle określonym przedziale czasu. Założeniem twórców aplikacji jest też przeniesienie części odpowiedzialności za właściwie zdefiniowany poziom uprawnień z administratora na właściciela danych – nikt nie jest w stanie lepiej określić niezbędnego poziomu dostępności do plików niż ich menedżer czy kierownik danego zespołu. Inną, nie mniej istotną funkcją pakietu oprogramowania jest możliwość przeprowadzania audytu i tworzenia dokumentacji w celu potwierdzenia zgodności z wdrożoną polityką bezpieczeństwa informacji, taką jak np. ISO 27000 czy PCI DSS.

> PRAKTYCZNE WTYCZKI

Standardowa funkcjonalność 8MAN może zostać rozszerzona za pomocą zestawu wtyczek. Dostępnych jest sześć pluginów nazwanych przez producenta: 8MATE for Exchange, for SharePoint, for vSphere, AD Logga, FS Logga oraz GrantMA.

8MATE for Exchange zgodnie z nazwą umożliwia rozszerzony wgląd w uprawnienia do obiektów charakteryzujących serwer pocztowy Microsoft, w tym uprawnienia do folderów



8MAN pozwala nie tylko na odczyt informacji o użytkownikach, możliwe jest również kompleksowe zarządzanie nimi.

publicznych, skrzynek pocztowych wraz z folderami i kalendarzy. Możliwe jest też namierzenie użytkowników mogących wysłać wiadomości e-mail w imieniu innych nadawców oraz identyfikowanie adresów z przekazywaniem wiadomości dalej. Podobnie jak w przypadku zarządzania uprawnieniami AD, wszystko dostępne jest z poziomu intuicyjnej konsoli graficznej. Wtyczka 8MATE for SharePoint w analogiczny sposób pozwala kontrolować uprawnienia przydzielane do elementów tej aplikacji wraz z raportowaniem zmian w zdefiniowanym przedziale czasu. Koncepcja kontroli dostępu definiowanej na poziomie właściciela danych sprawdza się również w delegacji uprawnień w tym środowisku. Dużą przejrzystością zarządzania systemem uprawnień charakteryzuje się też

oprogramowanie 8MAN dla systemów VMware vSphere.

Nowością w 6. wersji testowanego rozwiązania jest wtyczka dla systemów SAP (z adnotacją, że udostępniana jest na razie development partnerom). W praktyce jest to zapowiedź funkcji Open Connector umożliwiającej integrację z wieloma różnymi produktami dostępnymi na rynkach lokalnych, w tym polskim. Rozszerzenia AD Logga, FS Logga oraz GrantMA oferują następujące funkcjonalności. Zadaniem pierwszej z wtyczek jest dokumentacja wszystkich zmian w AD i generowanie raportów na podstawie zgromadzonych danych, z uwzględnieniem interesujących administratora ram czasowych. W raporcie można zawrzeć rodzaj zdarzenia, autora zmian, klasę obiektu oraz atrybuty z nim związane. Podobna funkcjonalność dostępna jest dla zasobów plikowych za pośrednictwem wtyczki FS Logga. Próby dostępu do zasobów zgromadzonych na serwerze, odczyty i modyfikacje plików oraz podgląd uprawnień to zdarzenia łatwo identyfikowalne dzięki raportom tworzonej za pomocą tej wtyczki. Ostatnim dostępnym pluginem jest 8MATE GrantMA – rozwiązanie odciążające administratorów domeny i pozwalające delegować część zadań związanych z przydzielaniem dostępu do zasobów na właściciela zasobu. W praktyce realizowane jest to za pośrednictwem portalu dostępnego z poziomu

**8MAN stworzono
w technologii .NET.
Ścisła integracja z AD
w połączeniu z intuicyjnym
interfejsem graficznym 8MAN
pozwalą na pełny monitoring
istniejącej struktury uprawnień
w administrowanym środowisku IT.**

przeglądarki internetowej, w którym pracownik wnioskuje o konkretne uprawnienia i członkostwo w danej grupie. W ten sposób odpowiedzialność za kontrolę nad poszczególnymi zasobami spada na osobę najbardziej zorientowaną w kwestii wrażliwości udostępnianych informacji oraz tego, kto powinien mieć do nich dostęp. W odróżnieniu od reszty wtyczek uruchomienie GrantMA wymaga dodatkowych czynności administracyjnych, w tym przystosowania usługi IIS.

> WYMAGANIA TECHNICZNE

Najnowsza, testowana przez nas wersja oprogramowania 8MAN oznaczona została numerem 6.0. Aby uzyskać dostęp do ograniczonej czasowo wersji trial programu, należy zarejestrować się na stronie producenta lub skontaktować się z dystrybutorem. Pierwszy sposób nie jest tylko formalnością, jak to bywa w przypadku większości producentów oprogramowania – dane podane podczas rejestracji są weryfikowane. Cała procedura może chwilę potrwać, a szybki, weekendowy test 8MAN prak-

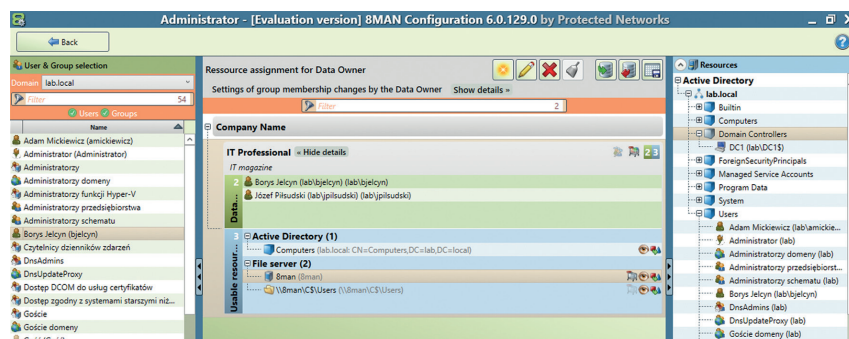


Konfiguracja ustawień aplikacji odbywa się z poziomu dedykowanego graficznego narzędzia 8MAN Configuration.

Wersja instalacyjna 8MAN zajmuje raptem 21 MB i udostępniana jest w postaci pojedynczego pliku wykonywalnego. Model wdrożenia bazuje na instalacji modułów funkcjonalnych na pojedynczym serwerze lub w środowisku rozproszonym. Podstawowe komponenty to: silnik bazodanowy MS SQL, 8MAN Server, 8MAN Collector oraz interfejs użytkownika. Pozostałe elementy, w tym opisane wcześniej wtyczki, są opcjonalne. Producent

konfiguracja bazuje na 4- lub 8-rdzeniowym CPU i 4-8 GB pamięci RAM na każdy komponent aplikacji. To niewiele. Wdrożenie można wykonać w środowisku fizycznym lub wirtualnym, pamiętając, iż nie jest zalecana wirtualizacja SQL Servera (obsługiwane są wersje SQL od 2008 SP1 do 2014). Wykorzystana może również zostać wersja silnika bazy danych SQL Express ograniczona limitami.

Komponent 8MAN Server, będący sercem systemu, oraz 8MAN Collector, a także interfejs użytkownika można uruchomić w systemach Windows Server, począwszy od wersji 2003 SP2 (obsługiwane są edycje 32- i 64-bitowe). Inaczej wygląda sytuacja dla pozostałych elementów – minimalna wersja systemu operacyjnego dla wtyczek to Windows Server 2008 w różnych wariantach (zależy od komponentu). Sama aplikacja 8MAN pozwala zarządzać uprawnieniami dla AD oraz usługi serwera plików, począwszy od wersji 2003. Wspomniane wcześniej wsparcie rozwiązań typu NAS dotyczy wersji oprogramowania Netapp ONTAP 7.3.1+ oraz EMC Celerra. Wspierany jest także DFS. Aby skorzystać z możliwości wtyczek dla Exchange oraz SharePoint, należy dysponować co najmniej wersjami 2007 obu aplikacji.



Wprowadzenie roli właściciela danych pozwala delegować część zadań administracyjnych na osoby zarządzające konkretnymi danymi.

tycznie nie wchodzi w grę. Instalację należy zaplanować z odpowiednim wyprzedzeniem, zwłaszcza że można spodziewać się kontaktu ze strony producenta. Podobnie wygląda sprawa dostępu do dokumentacji technicznej – na stronie WWW próżno szukać tutoriali czy forum użytkowników. Osoba zainteresowana produktem może otrzymać informacje tylko od producenta lub dystrybutora.

nie zdecydował się też na zintegrowanie z aplikacją silnika bazodanowego. Zadanie instalacji i konfiguracji MS SQL trzeba przeprowadzić we własnym zakresie. Skalowanie rozwiązania jest ściśle uzależnione od liczby użytkowników AD oraz serwerów plików. Producent podaje w dokumentacji przykładowe wymagania sprzętowe dla środowiska z 5000 użytkowników oraz 200 tys. folderów – rekomendowana

> INSTALACJA I OBSŁUGA

Sam proces instalacji to czynność wyjątkowo prosta – wystarczy wybrać komponenty, które powinny zostać zainstalowane, odhaczyć właściwe opcje,



+ wskazać folder instalacji oraz zaakceptować warunki licencji. Komponent 8MAN Server musi być instalowany tylko na jednym serwerze. Liczba interfejsów użytkownika oraz kolektorów jest dowolna. Jeśli instalator wykryje brak wymaganych komponentów systemowych, zaproponuje automatyczną instalację brakujących elementów. Po poprawnie zakończonej instalacji automatycznie uruchomiony zostaje 8MAN Configuration – graficzne narzędzie umożliwiające wstępną konfigurację całego środowiska, w tym danych uwierzytelniania, parametrów serwera MS SQL, pliku licencji oraz pozostałych ustawień systemowych. Z poziomu 8MAN Configuration należy również dodać wszelkie zasoby, do których prawami dostępu ma zarządzać 8MAN. Aby poznać szczegółowe opcje systemu, warto zerknąć do dokumentacji. Poradnik opisujący instalację i konfigurację 8MAN liczy niespełna 60 stron (z czego większość zajmują kolorowe rzuty ekranowe).

Po wstępnej konfiguracji parametrów można uruchomić właściwy program 8MAN. Podobnie jak w przypadku programu konfiguracyjnego mamy do czynienia z przejrzystym i czytelnym GUI (mimo to użytkownicy mający pierwszy raz do czynienia z rozwiązaniem tego typu będą musieli poświęcić chwilę, aby odnaleźć się w programie). Producent zadbał o to, aby

administracja uprawnieniami zarówno usługi katalogowej, jak i serwera plików była maksymalnie uproszczona i możliwie intuicyjna dla administratora. Dzięki mechanizmom przeciągnij i upuść oraz czytelnym matrycom uprawnień wprowadzanie zmian oraz weryfikacja dostępu na poziomie grup zajmują o wiele mniej czasu, aniżeli w przypadku wbudowanych mechanizmów Windows Server. Dostępne raporty mogą być wywoływane przez zdefiniowany harmonogram i doręczane bezpośrednio do skrzynki e-mail właściwego użytkownika.

Wdrożenie rozwiązania 8MAN nie jest procesem żmudnym i wymagającym. Już po kilku godzinach poświęconych na instalację, konfigurację oraz wstępne zapoznanie z możliwościami aplikacji możliwe jest generowanie wyczerpujących raportów na temat zarządzanego środowiska. Bardziej zaawansowany poziom administracji i użytkowania można osiągnąć po kilku dniach pracy z systemem. W zależności od wielkości zarządzanego środowiska i indywidualnych potrzeb wdrożyć możemy jedną z trzech wersji oprogramowania: 8MAN Visor, 8MAN Visor DO oraz 8MAN Enterprise. Pierwsza, najprostsza edycja umożliwia tylko odczyt informacji na jednym stanowisku. Wersja Visor DO pozwala na stworzenie rozproszonego środowiska, korzystanie z raportów bazujących

na harmonogramach oraz wprowadza funkcje związane z właścicielami danych. Wersja Enterprise nie ma żadnych ograniczeń funkcjonalnych i dedykowana jest najbardziej wymagającym klientom. Licencjonowanie produktu zależy od liczby użytkowników Active Directory. Aby właściwie dobrać wersję oprogramowania, konieczne jest skorzystanie z pomocy dystrybutora. Podobnie wygląda kwestia ustalenia ceny produktu – naturalnie im większy wolumen, tym niższy koszt jednostkowy licencji. W przypadku polskiego rynku polityka cenowa nie jest sztywna. Aby dostosować produkt do wymagań klienta, konieczny jest kontakt z dystrybutorem. **IT**

Autor jest architektem w międzynarodowej firmie z branży IT. Zajmuje się infrastrukturą sieciowo-serwerową, wirtualizacją infrastruktury i pamięcią masową.

PODSUMOWANIE

Systemy typu Access Rights Management, do których należy testowany 8MAN, to zestaw narzędzi, których głównym zadaniem jest ułatwienie wykonywania codziennych zadań związanych z kontrolą i zarządzaniem uprawnieniami użytkowników. Ważne w tym przypadku jest, na ile można uprościć cały żmudny proces kontroli dostępu,

tak aby ewentualna inwestycja w software miała sens. W przypadku oprogramowania 8MAN można zdecydowanie stwierdzić, że warto zainwestować w tego typu oprogramowanie, szczególnie wtedy, gdy mamy do czynienia ze środowiskiem liczącym setki, a nawet tysiące użytkowników. Jest to więc rozwiązanie przeznaczone dla średnich

oraz dużych klientów korporacyjnych, i tego typu organizacje najszybciej dostrzegą pozytywne efekty wynikające z jego wdrożenia. Oczywiście nic nie stoi na przeszkodzie, aby wdrożyć 8MAN w mniejszym środowisku – w tym przypadku warto jednak przeprowadzić szczegółową analizę zakresu potrzebnych funkcjonalności.

Werdykt

8MAN v. 6.0

Zalety

- + prosty i przejrzysty interfejs graficzny
- + skalowalność
- + wsparcie dla starszych wersji Windows Server
- + łatwe generowanie i dostosowywanie raportów
- + przejrzysty system zarządzania uprawnieniami

Wady

- wtyczka dla vSphere tylko dla wersji 5.0
- utrudniony dostęp do dokumentacji technicznej i wersji próbnej

Ocena



8/10