ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1997
Seria: INFORMATYKA z. 32 Nr kol. 1356

Andrzej KOWALCZYK, Arkadiusz TWARDOŃ, Robert WÓJCICKI
Politechnika Śląska, Instytut Informatyki

PRZEGLĄD WYBRANYCH NARZĘDZI POZWALAJĄCYCH NA ZARZĄDZANIE ZASOBAMI DOMENY SIECI MICROSOFT NETWORK

Streszczenie. W artykule zostały opisane popularne narzędzia programowe, służące do wspomagania procesu zdalnego zarządzania zasobami domeny sieci Microsoft Network oraz lokalnej i zdalnej konfiguracji stacji pracujących w obrębie takiej domeny.

THE REVIEW OF SELECTED TOOLS FOR MICROSOFT NETWORK DOMAIN RESOURCES MANAGEMENT

Summary. This article describes popular software tools, used to support the remote administration process of Microsoft Network domain resources with local and remote configuration of workstations connected to such domain.

1. Wstęp

We wstępie wyjaśnione zostało pojęcie *domeny* sieci Microsoft Network oraz przedstawiono podstawowe problemy związane z jej administracją.

1.1. Domena sieci Microsoft Network

Sieć Microsoft Network oferuje użytkownikowi wiele różnego typu zasobów. Należą do nich między innymi:

- konta użytkowników,
- współdzielone kartoteki i zbiory danych,

- współdzielone drukarki,
- oraz różnego typu procesy usługowe (ang. *services*).

Wyjaśnienia może wymagać termin "domena sieci". W sieci typu Microsoft Network pojęcie domena oznacza zbiór stacji roboczych oraz serwerów udostępniających sobie wzajemnie zasoby. Jeden z serwerów jest wyróżniony i pełni rolę kontrolera domeny (ang. *primary domain controller*), będąc odpowiedzialny za bezpieczeństwo pracy domeny (kontrola praw dostępu użytkowników do poszczególnych zasobów). Możliwe jest także zastosowanie dodatkowego kontrolera (ang. *backup domain controller*), którego zadaniem jest dublowanie pracy kontrolera podstawowego, tak aby w razie jego awarii móc przejąć na siebie ciężar zarządzania domeną. Należy tu podkreślić różnicę pomiędzy domeną a grupą roboczą (ang. *workgroup*), której zadaniem jest jedynie usprawnienie procesu nadawania użytkownikom praw do zasobów (w przypadku istnienia grup roboczych prawa dostępu mogą być nadawane wszystkim członkom grupy zarówno indywidualnie, jak i zbiorowo).

Ze względu na różne wymagania użytkowników i ich zróżnicowane możliwości korzystania z zasobów powstaje konieczność odpowiedniego zarządzania domeną sieci. Do najczęściej wykonywanych zadań administratora domeny należą:

- dodawanie i usuwanie kont użytkowników,
- tworzenie grup roboczych,
- kontrola i ewentualne zmiany uprawnień użytkowników i grup roboczych,
- dołączanie nowych i usuwanie istniejących zasobów,
- konfigurowanie komputerów pełniących rolę węzłów domeny.

1.2. Problemy administrowania domeną

Postęp w dziedzinie technologii tworzenia sieci komputerowych doprowadził do rozszerzenia się granic obszaru, w ramach którego sieć komputerowa uznawana jest za sieć lokalną. W ślad za tym zjawiskiem poszło zwiększenie liczby komputerów pracujących w obrębie takiej sieci. Obydwa te zjawiska doprowadziły do znacznego zwiększenia nakładu pracy administratora sieci, koniecznego do prawidłowego wywiązywania się z nałożonych na niego zadań. Istotne stało się również to, czy aby dla przeprowadzenia podstawowych prac administracyjnych (patrz punkt 1.1) administrator musi korzystać z określonego komputera (zwykle serwera), czy też może przeprowadzać te prace z dowolnego węzła sieci.

Biorąc pod uwagę powyższe stwierdzenia, w dalszej części artykułu postaramy się opisać, a następnie przeprowadzić analizę porównawczą wybranych narzędzi programowych, służących do administrowania domeną sieci MicrosofT Network.

2. Narzędzia pozwalające na zdalną administrację w sieci Microsoft Network

Ze względu na posiadane doświadczenie i możliwości sprzętowo-programowe do badań wybraliśmy sieć opartą na serwerze domenowym Microsoft NT wersji 3.51 oraz 4.0, i stacjach roboczych pracujących pod kontrolą systemu operacyjnego Windows 95.

Z myślą o zredukowaniu czasu traconego przez administratorów na przemieszczanie się pomiędzy węzłami i segmentami sieci firma Microsoft opracowała mechanizmy pozwalające na zdalne administrowanie zasobami domeny. Do mechanizmów tych należą: metody instalacji oprogramowania pozwalające na przyspieszenie i zautomatyzowanie procesu pierwotnego konfigurowania stacji roboczych oraz zestaw narzędzi pozwalających na zdalne zarządzanie w obrębie domeny.

Poniżej omówione zostaną tylko niektóre z wielu narzędzi programowych, pozwalające przeprowadzać zdalną konfigurację w środowisku sieciowym Microsoft Network.

Opis możliwości przedstawionych programów jest z konieczności skrócony (obszerność tematu), ale chcemy dodać, że wraz z oprogramowaniem dostarczana jest bogata dokumentacja. Opisuje ona zasady posługiwania się programami oraz przedstawia problemy związane z administrowaniem, jak również proponowane strategie ich pokonywania.

2.1. Remote registry

W systemie Windows 95 każdy użytkownik indywidualnie może określić niektóre parametry oraz sposób działania części składników systemu. Są to np. ustawienia interfejsu użytkownika, parametry dotyczące pracy w sieci, a także parametry niektórych aplikacji. Wszystkie te informacje są zapisywane w systemowej bazie danych registry.

Mimo że logicznie systemowa baza danych registry tworzy jedną strukturę, to fizycznie składa się z dwóch zbiorów: USER.DAT oraz SYSTEM.DAT. Zbiór USER.DAT zawiera informacje dotyczące indywidualnych ustawień poszczególnych użytkowników, podczas gdy w zbiorze SYSTEM.DAT zawarte są parametry wspólne dla wszystkich użytkowników danego komputera. Dlatego też, jeśli umożliwiono indywidualizację ustawień systemowych, każdy użytkownik posiada własny zbiór USER.DAT. Znajduje się on w podkatalogu $windir\Profiles\nazwa_użytkownika ($windir oznacza katalog, w którym jest zainstalowany system Windows 95).

Jednym z narzędzi służących do przeglądania i modyfikacji systemowych baz danych registry jest Registry Editor (REGEDIT.EXE). Edytor ten pozwala na lokalne oraz zdalne przeglądanie i modyfikację bazy registry użytkownika. Możliwość zdalnego zarządzania

registry jest często wykorzystywana przez administratorów sieci Microsoft Network, zwłaszcza w przypadku rozbudowanej sieci komputerowej.

Registry Editor przedstawia hierarchiczną zawartość systemowej bazy danych registry w postaci drzewa. Na najwyższym poziomie hierarchii znajduje się sześć głównych kluczy:

- Hkey_Local_Machine - zawiera informacje związane z zainstalowanymi urządzeniami, ustawieniami oprogramowania oraz inne. Te informacje dotyczą wszystkich użytkowników danego komputera.
- Hkey_Current_Config - wskazuje na gałąź Hkey_Local_Machine\Config, gdzie są przechowywane informacje o aktualnej sprzętowej konfiguracji komputera.
- Hkey_Dyn_Data - wskazuje na gałąź Hkey_Local_Machine, w której znajdują się dynamicznie zmieniane informacje o urządzeniach Plug and Play. Informacje te mogą się zmieniać w zależności od tego, czy dane urządzenie zostało umieszczone bądź wyjęte z komputera.
- Hkey_Classes_Root - odwołuje się do miejsca w Hkey_Local_Machine, w którym znajdują się ustawienia aktualnie zainstalowanego oprogramowania. Są tu np. wyświetlane informacje dotyczące OLE, operacji drag-and-drop, skrótów Windows 95 oraz części ustawień interfejsu użytkownika.
- Hkey_Users - zawiera informacje o wszystkich użytkownikach logujących się do danego komputera, jak np. domyślne ustawienia aplikacji, konfiguracje pulpitu i inne. Na podstawie tych informacji tworzony jest profil użytkownika.
- Hkey_Current_User - odwołuje się do klucza w Hkey_Users, który wskazuje dane bieżącego użytkownika.

Poszczególne klucze hierarchii zawierają gałęzie podrzędne, aż do miejsca, w którym ustawiana jest wartość bądź binarna, bądź w postaci ciągu znaków.

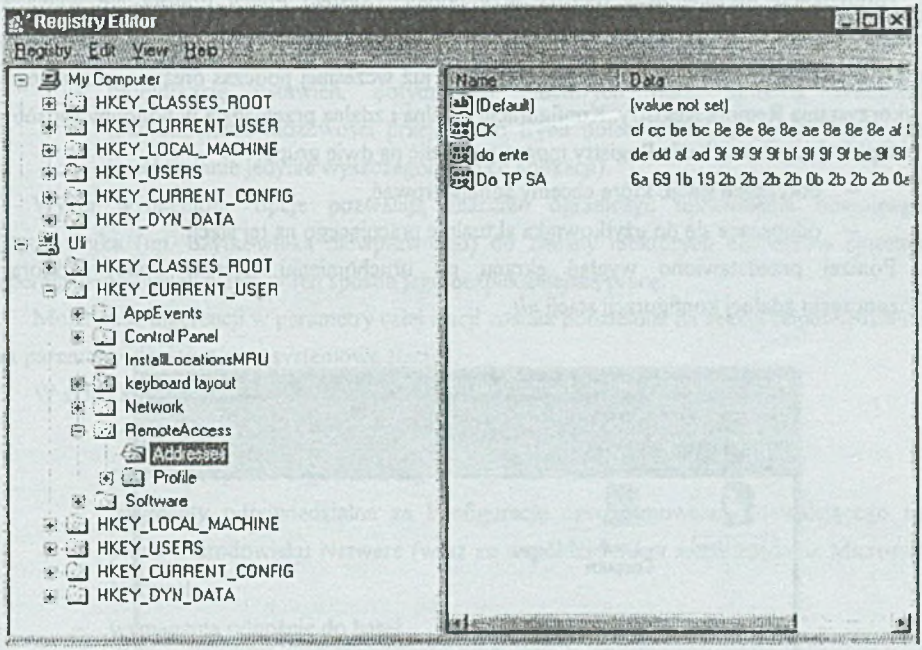
W odróżnieniu od narzędzia System Policy Editor, Registry Editor umożliwia pełną edycję bazy registry tzn. modyfikowanie wszystkich istniejących kluczy, dodawanie nowych, usuwanie już istniejących oraz zmianę wartości im przypisanych. Jak już wcześniej wspomniano, pozwala również na zdalne przeglądanie i modyfikowanie bazy registry. Jednak, by można było użyć zdalnego dostępu do bazy registry, należy wykonać kilka poniżej podanych czynności:

- zainstalować usługę Microsoft Remote Registry,
- uaktywnić opcję zezwalającą na zdalne zarządzanie systemem (opcja Password w Control Panel),
- na wszystkich zdalnie zarządzanych komputerach włączyć system ochrony na poziomie użytkowników (user-level security).

Dodatkowo trzeba spełnić jeszcze kilka warunków:

- wszystkie komputery podlegające zdalnemu zarządzaniu powinny posiadać wspólny protokół sieciowy,
- w sieci powinien pracować serwer Windows NT lub NetWare (związane jest to z systemem ochrony na poziomie użytkowników).

Jeżeli zostały spełnione wyżej wymienione warunki, można wtedy, m. in. za pomocą narzędzia Registry Editor, zdalnie zarządzać systemową bazą danych registry. Zasady zdalnego zarządzania są analogiczne jak podczas pracy lokalnej.



Rys. 1. Hierarchiczna struktura systemowej bazy danych Registry przedstawiona za pomocą narzędzia Registry Editor

Fig. 1. Hierarchical structure of Registry data base shown by Registry Editor

Powyżej przedstawiona została przykładowa sesja z narzędziem Registry Editor, podczas zdalnego zarządzania bazą registry stacji roboczej o nazwie *uli*. Na rysunku widać również, w jaki sposób przedstawiona jest hierarchiczna struktura registry zarówno dla stacji lokalnej, jak i zarządzanej zdalnie.

2.2. System Policy Editor

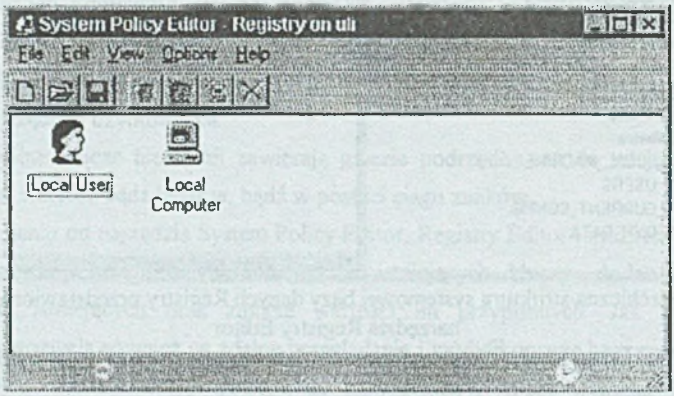
System Policy Editor to kolejne narzędzie programowe, umożliwiające ingerencje zarówno w lokalne, jak i zdalne bazy registry. W odróżnieniu od Registry Editora pozwala on jedynie na modyfikację niektórych elementów bazy registry, umożliwiając jednak tworzenie zestawów uprawnień nadawanych poszczególnym użytkownikom lub ich grupom (zbiór CONFIG.POL), a przechowywanych na serwerze, co znacznie upraszcza proces zdalnej konfiguracji sieciowej. Dodatkowo uprawnienia nadawane odgórnie (zbiór CONFIG.POL) przykrywają uprawnienia wynikające z ustawień lokalnych.

Modyfikacja lokalnej bazy registry przy pomocy System Policy Editora nie wymaga żadnych dodatkowych zabiegów, jeżeli jednak chcemy, aby możliwa była konfiguracja zdalna, to niezbędne jest spełnienie warunków, opisanych już wcześniej podczas omawiania zdalnego wykorzystania Remote Registry. Konfiguracje lokalna i zdalna przebiegają w podobny sposób.

Operacje zmian w bazie Registry można podzielić na dwie grupy:

- dotyczące stacji, którą chcemy administrować,
- odnoszące się do użytkownika aktualnie pracującego na tej stacji.

Poniżej przedstawiono wygląd ekranu po uruchomieniu System Policy Editora, i rozpoczęciu zdalnej konfiguracji stacji *uli*.



Rys. 2. Otwarte okno System Policy Editora dla stacji roboczej *uli*
Fig. 2. Opened System Policy Editor windows for *uli* workstation

Jak widać, możliwa jest ingerencja zarówno w ustawienia dotyczące aktualnie pracującego tam użytkownika (ikona Local User), jak i w ustawienia samej stacji roboczej (ikona Local Computer).

Wybór pierwszej możliwości (użytkownik) pozwala na wykonywanie następujących operacji:

- blokowanie dostępu użytkownika do niektórych opcji panelu sterowania (sekcje Display, Network, Passwords, System i Printers),
- ingerencję w wygląd Desktopu (wybór tapety oraz schematu kolorystycznego),
- blokadę uprawnień pozwalających udostępniać zasoby współdzielone (zbiory i drukarki),
- zmianę parametrów shella systemu Windows (sekcja dotycząca folderów zawierających: programy, ikony rozmieszczone na Desktopie, aplikacje uruchamiane podczas startu systemu, stacje włączone do sieci, zawartość Start Menu oraz sekcja restrykcji, polegających między innymi na zablokowaniu polecenia Run w menu startowym, dostępu do sieci, wyłączeniu możliwości zamknięcia systemu),
- modyfikację ustawień, dotyczących niektórych opcji systemu Windows (zablokowanie możliwości przejścia do trybu poleceń DOSa, lub też zgoda na uruchamianie jedynie wyszczególnionych aplikacji).

Wyżej wymienione opcje pozwalają znacznie ograniczyć uprawnienia dowolnego użytkownika (np. użytkownika niewprawnego) do zmiany niektórych elementów systemu operacyjnego, zapewniając w ten sposób jego bezpieczniejszą pracę.

Możliwość ingerencji w parametry całej stacji została podzielona na sekcje odpowiedzialne za parametry sieciowe oraz systemowe stacji.

W skład sekcji sieciowej wchodzą kolejno:

- tryb dostępu do zasobów współdzielonych,
- przebieg i sposób logowania się,
- fragmenty odpowiedzialne za konfigurację oprogramowania pozwalającego na pracę w środowisku Netware (wraz ze współdzieleniem zasobów) oraz Microsoft Network,
- wymagania odnośnie do haseł,
- możliwość zablokowania korzystania z modemu,
- udostępnianie lub nie zasobów współdzielonych (zbiory i drukarki),
- fragment odpowiedzialny za konfigurację SNMP,
- oraz opcja pozwalająca na zdalne (na serwerze) uaktualnianie zawartości bazy Registry.

Elementy sekcji systemowej pozwalają na dokonywanie następujących operacji:

- zgoda na własne profile wszystkich użytkowników korzystających ze stacji,
- określenie ścieżki systemowej zbioru konfiguracyjnego systemu Windows (Windows Setup) oraz zbioru zawierającego krótki samouczek systemu Windows (Windows Tour),

- fragment odpowiedzialny za aplikacje i usługi uruchamiane każdorazowo podczas startu systemu oraz aplikacje uruchamiane podczas startu systemu jednorazowo.

Podsumowując można powiedzieć, że System Policy Editor pozwala na szybką i wygodną konfigurację (zwłaszcza zdalną) niektórych elementów baz registry użytkowników pracujących w sieci, co w znacznym stopniu przyczynia się do zwiększenia efektywności i komfortu pracy administratora. Godne polecenia wydaje się stosowanie tego narzędzia zwłaszcza wtedy, gdy narzuciliśmy obowiązkową weryfikację haseł przez serwer domenowy. Możemy w ten sposób doprowadzić do sytuacji, w której bez podania hasła konkretny użytkownik (lub grupa użytkowników) będzie pozbawiony możliwości pracy tylko i wyłącznie lokalnej, a po jego podaniu i weryfikacji przez serwer dostęp do określonych zasobów i/lub możliwości wykonywania wyszczególnionych zadań (programów) będzie odpowiednio ograniczony.

2.3. Event Viewer

Event Viewer jest narzędziem pozwalającym na obserwowanie, jakie zdarzenia wystąpiły w analizowanym węźle w pewnym okresie czasu. Rejestrowane w węźle zdarzenia podzielone są na kategorie tematyczne. Możliwe jest przeglądanie rejestrów zdarzeń dla:

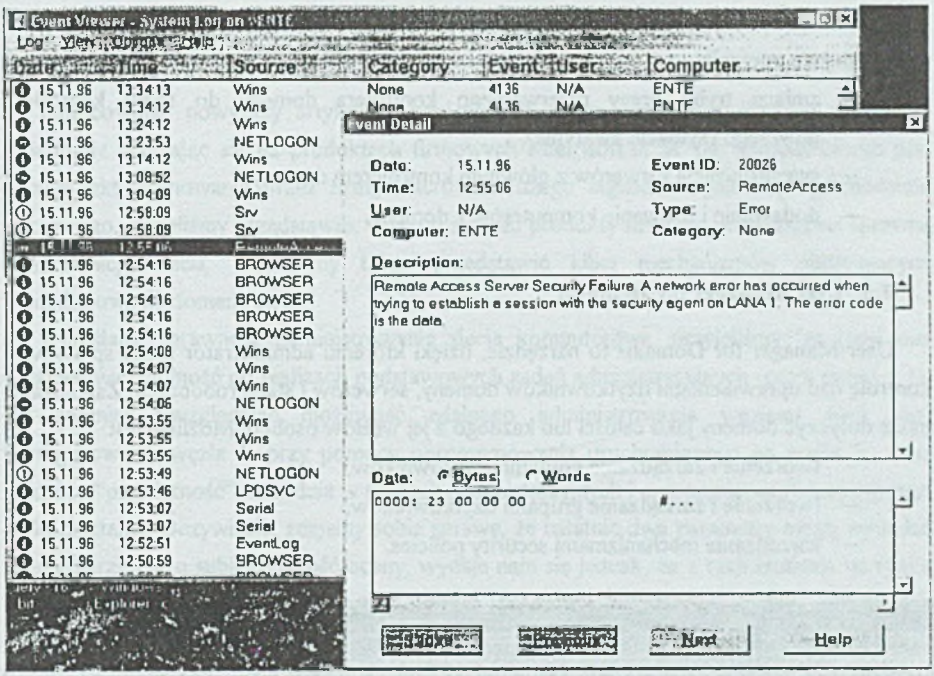
- systemu,
- aplikacji,
- poziomu kontroli uprawnień.

Podobnie jak pozostałe, opisane poniżej, narzędzia Event Viewer pozwala na połączenie się z analizowanym systemem za pomocą łącz powolnych, jak i sieci lokalnej. Dzięki tej możliwości administrator ma dostęp do maszyn znacznie oddalonych w przestrzeni od miejsca jego pracy, co doskonale podnosi użyteczność opisywanego narzędzia

Zdarzenia warstwy systemowej podzielone są na trzy kategorie:

- zdarzenia o charakterze informacyjnym,
- zdarzenia o charakterze ostrzegawczym,
- zdarzenia krytyczne dla integralności systemu.

W zależności od wagi zdarzenia opatrzone ono zostaje bądź znakiem "i", bądź znakiem "!", bądź też napisem "STOP".



Rys. 3. Okno Event Viewer'a zawierające informacje o zdarzeniach warstwy systemu wraz z opisem jednego ze zdarzeń

Fig. 3. Event Viewer window shows system log with detailed description of one event

2.4. Server Manager

Server Manager to narzędzie, które umożliwia zarządzanie zasobami udostępnianymi w obrębie domeny. Pozwala też na konfigurowanie oprogramowania systemowego pracującego na komputerach pełniących rolę węzłów sieci.

W wypadku administrowania komputerem-węzłem sieci Server Manager umożliwia:

- obserwowanie listy użytkowników korzystających z zasobów udostępnianych przez węzeł,
- zarządzanie mechanizmem replikowania kartotek,
- definiowanie listy użytkowników, do których mają być rozsyłane informacje o zaistnieniu sytuacji alarmowej,
- zmianę parametrów procesów usługowymi pracującymi w węźle,
- zarządzanie system udostępnianych kartotek,
- rozsyłanie komunikatów do użytkowników podłączonych do węzła.

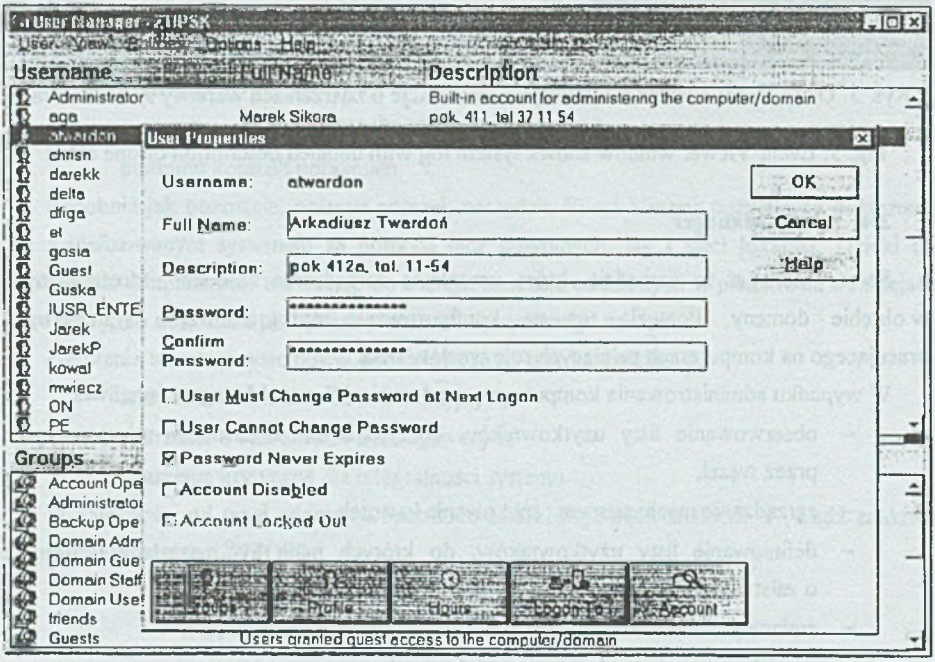
Jeśli administrujemy domeną sieci przy użyciu Server Managera, to możliwe do wykonania są następujące operacje:

- zmiana trybu pracy rezerwowego kontrolera domeny do trybu kontrolera głównego (sytuacje awaryjne),
- synchronizacja serwerów z głównym kontrolerem domeny,
- dodawanie i usuwanie komputerów z domeny.

2.5. User Manager for Domains

User Manager for Domains to narzędzie, dzięki któremu administrator może sprawować kontrolę nad uprawnieniami użytkowników domeny, serwerów i stacji roboczych. Zarządzanie może dotyczyć domeny jako całości lub każdego z jej węzłów osobno. Możliwe jest:

- tworzenie i zarządzanie kontami użytkowników,
- tworzenie i zarządzanie grupami użytkowników,
- zarządzanie mechanizmami security policies.



Rys. 4. Okno programu User Manager wraz z opisem użytkownika *atwardon*
Fig. 4. User Manager window with *atwardon* account properties

3. Wnioski końcowe

Opracowując powyższy artykuł, z konieczności wybraliśmy tylko niektóre narzędzia, świadomie skupiając się na produktach firmowych Microsoft'u. W ten sposób, biorąc pod uwagę fakt opanowania przez firmę Microsoft dużego segmentu rynku oprogramowania sieciowego, chcieliśmy przedstawić, w jakim stopniu produkty firmowe pozwalają na sprawną administrację siecią. Chcieliśmy także przedstawić kilka mechanizmów ułatwiających administrowanie domeną sieci.

Określając sprawność administrowania siecią komputerową, przyjęliśmy, że musi ona uwzględniać zdolność do realizacji podstawowych zadań administracyjnych (patrz punkt 1.1), jak również uwzględniać możliwość zdalnego administrowania węzłami sieci, tzn. konfigurowania węzła X przy pomocy oprogramowania uruchomionego na węźle Y, oraz w końcu "przydatność" narzędzia w pracach administracyjnych i ergonomię, czyli łatwość jego wykorzystania. Oczywiście, zdajemy sobie sprawę, że ostatnie dwa parametry mogą wywołać szereg zarzutów o subiektywność oceny, wydaje nam się jednak, że z racji istnienia na rynku wielu podobnych aplikacji warto ocenić produkty oferowane przez producenta oprogramowania systemowego.

Przechodząc do komentarza, to po pierwsze widać, że wybrane przez nas aplikacje dzielą się na dwie grupy: służące do monitorowania oraz strojenia systemu. Monitorowanie pracy węzłów sieci pozwala na wyodrębnienie parametrów i fragmentów podglądanego systemu krytycznych dla wydajności i bezpieczeństwa pracy w sieci oraz pracy lokalnej. Dzięki temu pomoc narzędzi konfigurujących oprogramowanie systemowe możliwe jest takie dopasowanie wartości tychże parametrów, które pozwala na optymalne wykorzystywanie zasobów oferowanych przez domenę sieci.

Narzędzia takie jak User Manager for Domain, Server Manager oraz Event Viewer mają swoje odpowiedniki wśród programów wchodzących w skład systemów Windows NT Server i Windows NT Workstation, jednakże odpowiedniki te pozwalają na zarządzanie tylko i wyłącznie zasobami maszyny, na której zostały uruchomione. W przeciwieństwie do nich omawiane przez nas narzędzia pozwalają na administrację wszystkimi komputerami pełniącymi rolę węzłów sieci, niezależnie od tego, w którym węźle zostały faktycznie uruchomione. Dla platformy Windows 95 narzędziami pozwalającymi na zdalne monitorowanie i konfigurację węzła sieci są: System Policy Editor oraz Registry Editor, wykorzystujący mechanizm Remote Registry. Biorąc pod uwagę rozległość współczesnych sieci oraz liczbę węzłów w nich pracujących, trzeba stwierdzić, że możliwość zdalnego administrowania każdym węzłem z jednego miejsca wydaje się dużym ułatwieniem w pracy administratora sieci Microsoft

Network i wobec tego znacznie poprawia sprawność administrowania sieciami lokalnymi tego typu.

LITERATURA

[1] Windows 95 User's Guide, Microsoft Corporation 1995.
[2] Windows NT System Guide, Microsoft Corporation 1995.
[3] Microsoft Windows 95 Resource Kit, Microsoft Press 1995.

Recenzent: Dr inż. Ryszard Winiarczyk

Wpłynęło do Redakcji 18 listopada 1996 r.

Abstract

This article describes the software tools used to support the process of remote and local administration of Microsoft Network domain resources.

As far as the network administration is concerned, we all know that this problem broadens every year, with new products and tools development. All world leading companies give us a plenty of new software utilities, but it is sometimes very difficult to decide which one to choose.

We have described Microsoft products, because for the last 3 years we have been conducting thorough researches on its products (Windows NT, Windows 3.11 and Windows 95 operating systems with tools and utilities), so we have a considerable experience in this field. Besides that Microsoft has great shares in the software market, thus having also a very big influence on world software development tendencies.

In the first chapter we have described the idea of a *domain* (according to Microsoft specification) and shared resources with all problems connected with administrator's everyday routine.

Software tools used during Microsoft Network remote administration process have been shortly described in chapter two. We have chosen only very popular and easy accessible tools, like: *Registry Editor*, *System Policy Editor*, *Event Viewer*, *Server Manager* and *User Manager for Domains*, which are often used by domain administrators.

In each subchapter we have given a short description of one tool, including some figures illustrating the main aspects of its usage. We also tried to give clues on the most important facts about the products itself.

The last chapter gives a brief summary with our opinions about the above mentioned software.