IT Professional, 01/2019, Novell NetStorage

Dostęp do plików i folderów serwerów Linux za pomocą WWW

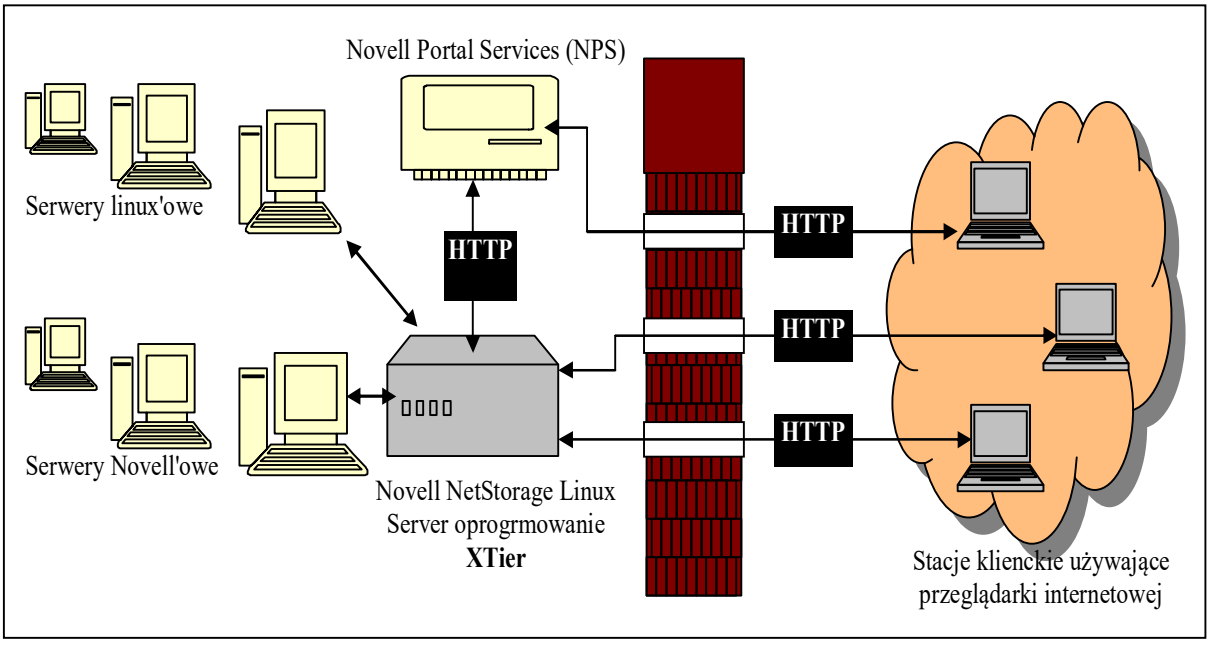
Wraz z instalacją usługi *Novell NetStorage* na serwerowym systemie operacyjnym *Micro Focus Open Enterprise Server 2018 (OES)* użytkownicy uzyskali dostęp do swoich folderów i plików znajdujących się na dowolnych serwerach typu *Linux* i *NetWare 5* (lub późniejszych) zlokalizowanych gdziekolwiek w firmowej/korporacyjnej rozproszonej sieci komputerowej.

Zygmunt Bok

Autentykacja użytkownika w usłudze *Novell NetStorage* bazuje na bardzo silnej usłudze katalogowej ***NetIQ eDirectory***. Dzięki niej dostęp za pomocą zwykłej przeglądarki (typu *Internet-based)* do folderów i plików zlokalizowanych na serwerach *netware*'owych lub *linu*ksowych jest tak bezpieczny jak dostęp do nich ze stacji roboczej użytkownika z poziomu sieci lokalnej *LAN*.

> ZASADA DZIAŁANIA USŁUGI *NOVELL NETSTORAGE*

Usługa *Novell NetStorage* działa jako serwer typu *Middle Tier,* znany również jako *XTier*, który pokazano na %%**rys. 1**%%. Po jego zainstalowaniu i konfiguracji *Novell NetStorage* prezentuje się dla użytkownika jak serwer typu *Internet Web* dostępny za pomocą przeglądarek internetowych, wyświetlający foldery i pliki będące do dyspozycji dla danego użytkownika.



Rys. 1. Zasada działania serwera typu *Middle Tier*.

Kiedy użytkownik zamierza uzyskać dostęp do swoich folderów i plików zlokalizowanych na serwerach typu *NetWare* w sieci lokalnej *LAN,* usługa *NetStorage* czyta: 1) skrypt logujący (*login script*) użytkownika – w celu określenia poleceń mapujących (*MAP*) sieciowe napędy dyskowe, 2) własności obiektu użytkownika z drzewa katalogowego ***NetIQ eDirectory*** – w celu określenia ścieżki do domowego folderu użytkownika i na podstawie tej informacji wyświetlenia listy dostępnych folderów oraz plików.

W sytuacji, kiedy użytkownik zamierza uzyskać dostęp do folderów i plików na serwerach typu *Linux*, usługa *NetStorage* czyta niezbędne informacje zawarte we właściwościach instancji obiektu typu *Storage Location Object*, do którego użytkownik ma prawa czytania (*Read*), zlokalizowanego w hierarchicznej strukturze katalogu *eDirectory*. Po odczytaniu tych danych *NetStorage* wyświetla dostępne dla tego użytkownika i stowarzyszone z tym obiektem katalogi z serwera *linuks*owego. Informacje konfiguracyjne tego serwera są magazynowane w pliku typu *XML*. W celu zwiększenia bezpieczeństwa wszystkie transakcje mogą być szyfrowane poprzez używanie protokołu *SSL*.

Mimo że użytkownik ma nadane przez administratora właściwe prawa obiektowe (*eDirectory rights*) do pewnych folderów i plików na serwerze, nie może uzyskać do nich dostępu, chyba że istnieją dla nich: 1) odpowiednie polecenia mapujące zawarte w skrypcie logującym, 2) foldery znajdujące się w katalogu domowym użytkownika, określone w obiekcie typu *Storage Location*.

Serwer *Middle Tier* komunikuje się w sieci lokalnej *LAN* z serwerami typu *NetWare* lub *Linux*, zapewniając bezpieczną autentykację za pomocą usługi *NetIQ eDirectory*.

> USŁUGA KATALOGOWA *NETIQ eDirectory*

Wśród dostępnych na rynku usług katalogowych znajduje się *NetIQ eDirectory*. *Popr*zednio, tj. od wersji systemu operacyjnego *NetWare* 4.00 (1993 r.), usługę tę nazywano *NDS (NetWare Directory Services),* później – wraz z systemem *NetWare* 5.0 (1998 r.) – przekształcono jej nazwę na *Novell Directory Services*. Od wersji systemu operacyjnego *NetWare* 6.0 (2001 r.) *NDS* został przemianowany na usługę *eDirectory* (wstępny opis w „IT Professional" 6/2018, s. 32).

Usługa katalogowa określa sposób zorganizowania całej sieci komputerowej przedstawionej w sposób hierarchiczny, zgodnie z założeniami organizacji lub korporacji, dla której została zaimplementowana. Usługa katalogowa stanowi pewną bazę informacyjną, korzystającą ze zróżnicowanych typów informacji o użytkownikach i zasobach komputerowych w środowisku sieciowym. W środowisku systemów operacyjnych *Netware*, *eDirectory* jest obiektowo zorientowaną implementacją tej bazy informacyjnej, przechowującą informacje o wszystkich obiektach znajdujących się w sieci. Usługa *eDirectory* w literaturze informatycznej określana jest jako obiektowo zorientowana baza danych. W związku z tym, że w dostępnej autorowi literaturze brak

jest odnośników uzasadniających powyższe stwierdzenie w tym sensie, że baza ta spełnia wszystkie wymagania stawiane obiektowym bazom danych, dlatego też w niniejszym artykule używać się będzie określenia „*eDirectory* będące obiektowo zorientowaną implementacją bazy informacyjnej, tj. usług katalogowych" - w skrócie „Katalogową bazą *eDirectory*".

Istnieje kilka aspektów, które różnią tradycyjną usługę katalogową od relacyjnej bazy danych. W zależności od aplikacji katalogowej informacje są o wiele częściej czytane niż zapisywane. W związku z tym zalety relacyjnej bazy danych, takie jak *rollback* czy transakcje, w niektórych usługach katalogowych nie są nawet zaimplementowane. Wymogiem nadrzędnym stawianym usługom katalogowym jest szybsza odpowiedź podczas wyszukiwania danych, które odbywa się na podstawie atrybutów danych, a następnie odczytywane są ich wartości. Schemat usługi katalogowej jest zdefiniowany w postaci klas obiektowych, atrybutów i danych. W poprzednich wersjach sieciowych systemów operacyjnych *NetWare* używano do przechowywania informacji o pojedynczym serwerze sieciowym płaskiej bazy danych zwanej *bindery*, charakteryzującej się tym, że poszczególne pozycje w tej bazie nie mają bezpośrednich wzajemnych związków z innymi pozycjami.

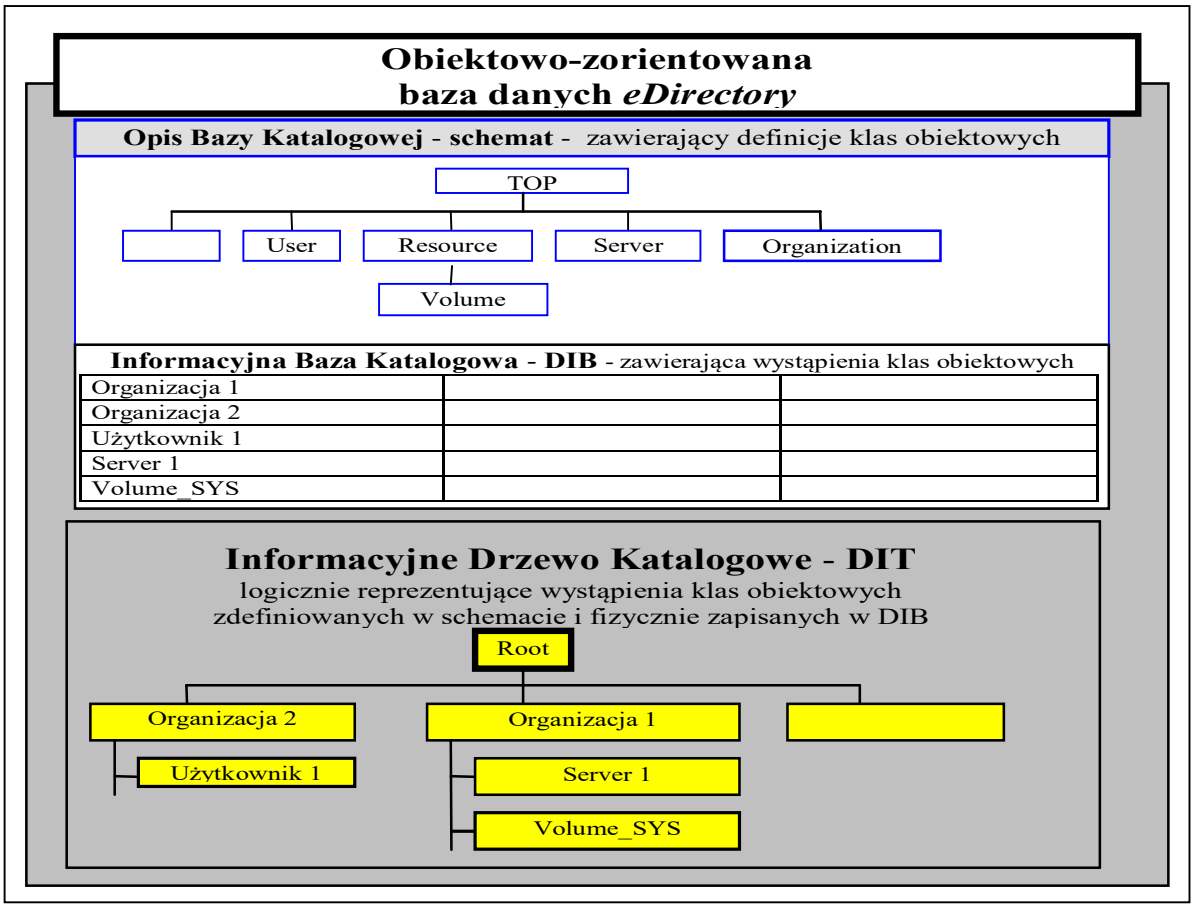
W przeciwieństwie do bazy *bindery*, strukturę *eDirectory* zorganizowano hierarchicznie. Widać w niej związki pomiędzy obiektami i stanowi ona globalną, rozproszoną oraz replikowaną obiektowo zorientowaną bazę danych, przechowującą informacje o wszystkich zasobach sieciowych, takich jak użytkownicy, grupy, serwery, woluminy, drukarki, komputery czy modemy. Przez pojęcie rozproszonej bazy danych *eDirectory* rozumie się zbiór węzłów (serwerów) połączonych siecią komunikacyjną, na których zainstalowano lokalne systemy baz danych *eDirectory*.

W sieciach złożonych z kilku serwerów partycja główna (*Master*) lub główna część bazy *eDirectory* rezyduje na pewnym wyróżnionym serwerze sieciowym, natomiast pozostałe jej partycje znajdują się na innych serwerach. W rzeczywistości rozproszona i replikowana na innych serwerach sieciowych jest baza *Directory Information Base* (*DIB)*, która opisuje katalogową bazę *eDirectory* i jej pliki, natomiast utrzymywana i zarządzana jest przez usługę *eDirectory*. W celu zapewnienia bezpieczeństwa i niezawodności wszystkie partycje są replikowane i przechowywane na sąsiednich serwerach włączonych do sieci komputerowej. Miejsce składowania plików całej bazy *eDirectory* lub poszczególnych jej partycji to katalog *SYS:NETWARE*, który znajduje się na każdym z serwerów sieciowych *NetWare*, a jest niedostępny dla użytkowników pracujących na stacjach roboczych w sieci *LAN*.

eDirectory opracowano w taki sposób, aby można było tworzyć hierarchiczną strukturę tzw. drzewa katalogowego (*Directory Tree*), składającego się z jednostek organizacyjnych zawierających użytkowników i komputerowe zasoby sieciowe. Zasady definiujące konstrukcję drzewa katalogowego określono i zapisano w postaci odpowiednich klas obiektowych, w hierarchicznym

opisie bazy katalogowej (*Directory Schema*) lub inaczej – na schemacie. Obiektowo zorientowana baza *eDirectory*, której budowę przedstawiono na %%rys. 2%%, jest logicznie reprezentowana przez hierarchiczną strukturę informacyjnego drzewa katalogowego (*Directory Information Tree – DIT*) , zawierającego różne pozycje.

Każda pozycja w informacyjnym drzewie katalogowym (*DIT)* odpowiada fizycznym pozycjom (tj. wystąpieniom pewnej klasy obiektowej) zawartym w informacyjnej bazie katalogowej (*Directory Information Base – DIB*), która jest jego fizyczną reprezentacją. Innymi słowy, schemat *eDirectory*, jako zbiór klas obiektowych, określa rodzaje obiektów, jakie można dodawać do informacyjnej bazy katalogowej (*DIB*), której rekordy są logicznie reprezentowane przez informacyjne drzewo katalogowe (*DIT*).



Rys. 2. Schematyczne przedstawienie budowy obiektowo zorientowanej bazy *eDirectory.*

Dla użytkowników sieci komputerowej jest wiele korzyści, jakie wynikają ze stosowania *eDirectory*. Począwszy od prostego aktu logowania się do całej sieci komputerowej – a nie tylko do pojedynczego serwera sieciowego – umożliwiającego łatwiejszą nawigację po zasobach sieciowych i czerpanie z nich przez autoryzowanych użytkowników, poprzez szerokie korzystanie z dostępnych

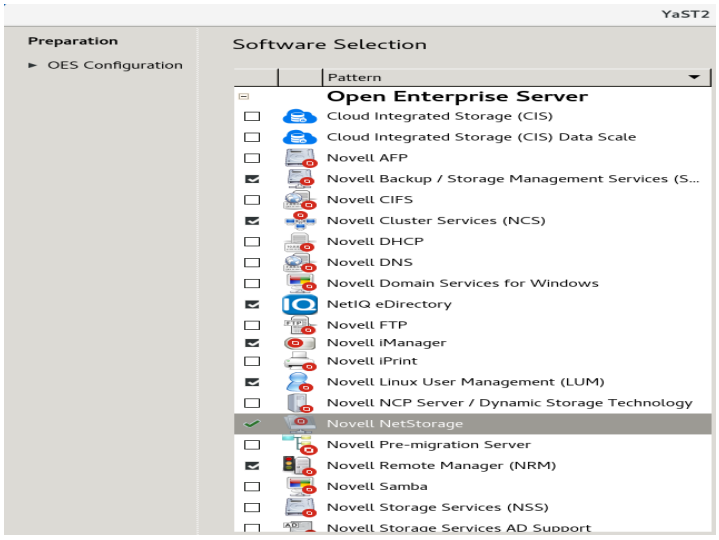
usług sieciowych bez konieczności znajomości topologii sieci (*eDirectory* jest niezależna od platformy topologicznej), protokołów, mediów transmisyjnych i połączeń komunikacyjnych, aż po dostęp do sieci internetowej.

> INSTALACJA I KONFIGURACJA USŁUGI *NOVELL NETSTORAGE*

W celu zainstalowania usługi *NetStorage* muszą być spełnione niezbędne wymagania: 1) zainstalowanie w sieci *LAN* usługi katalogowej *NetIQ eDirectory*, 2) zainstalowanie w sieci *LAN*, w części serwerowej usługi *NetStorage*, przynajmniej jednego serwera *OES* znajdującego się w strukturze drzewa katalogowego *NetIQ eDirectory*, na którym będzie instalowana usługa *NetStorage*, 3) zainstalowanie w części klienckiej usługi *NetStorage*, na stacji roboczej w sieci *LAN*, przeglądarki typu *Internet Explorer*, *Mozilla*, *Safari* lub innej przeglądarki *linu*ksowej.

Usługa *NetStorage* w części serwerowej jest instalowana oraz wstępnie konfigurowana przy użyciu domyślnych ustawień, które można zmienić podczas instalacji systemu operacyjnego *SUSE Linux Enterprise Server (SLES) 12 SP2*. Usługę można też zainstalować później, co pokazano na %%rys. 3%%. Wówczas należy:

1) zalogować się do tego serwera jako użytkownik *root*,
2) otworzyć program administracyjny *YaST*, a następnie wybrać opcję <<*Open Enterprise Server*>> *i* <<*OES Install and Configuration*>>,
3) na stronie <<*OES Services Configuration*>> zaznaczyć <<*Novell NetStorage configuration*>>.

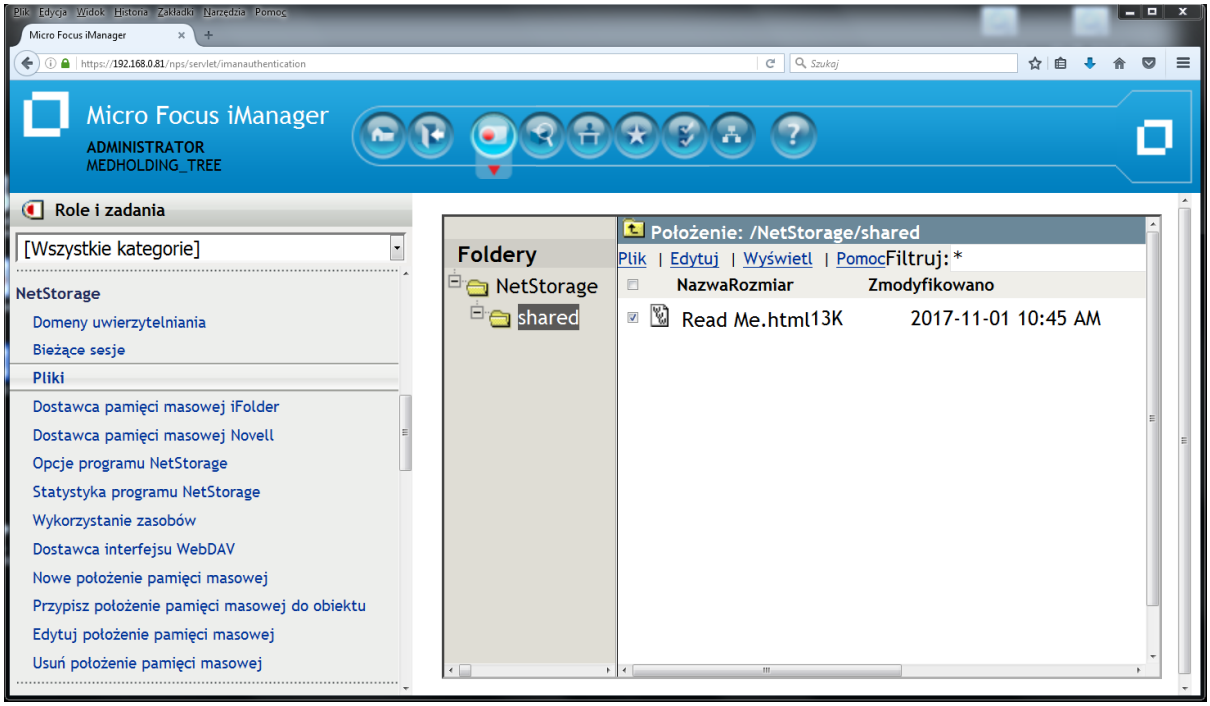


Rys. 3. Instalacja serwerowej części usługi *Novell NetStorage.*

Po zainstalowaniu *Novell NetStorage* użytkownik może zobaczyć tylko współdzielone katalogi na serwerze *linu*ksowym (*OES)* w przeglądarce internetowej łączącej się z serwerem *OES* za pomocą *web*owego programu *Micro Focus iManager* z systemu *Micro Focus Open Enterprise Server 2018 (*%%rys. 4%%). W celu uzyskania dostępu do katalogów i plików na tym serwerze wymagane jest

utworzenie i skonfigurowanie obiektu typu ***Storage Location Object***, chyba że na serwerze *OES* zainstalowano serwerowy komponent *NCP* (*NetWare Core Protocol*).

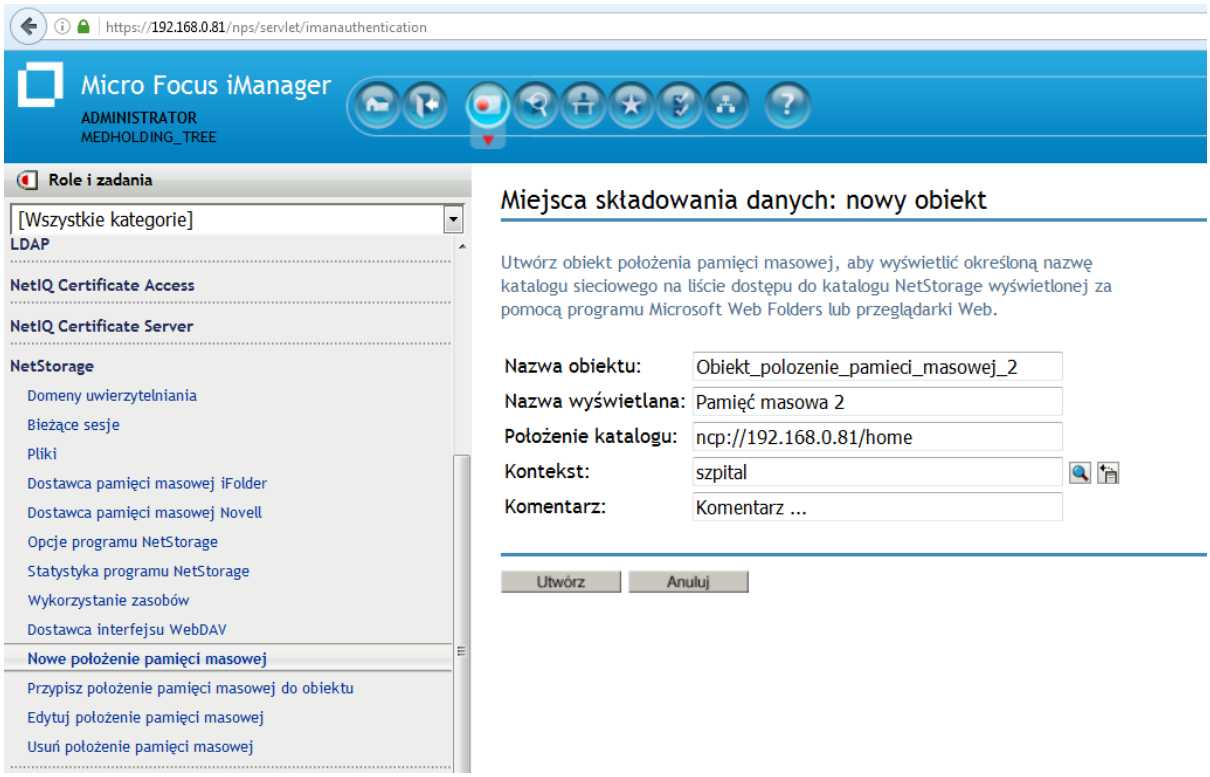
W usłudze *NetStorage* zaimplementowano metodę dostępu do folderów i plików, za pomocą protokołu *SSH* (*Secure Shell*), pozwalającego na dostęp do plików w systemach *linu*ksowych, które nie wspierają protokołów *NCP* lub *CIFS*. Z protokołu *SSH* można korzystać dzięki utworzonemu obiektowi *typu eDirectory Storage Location* wraz z właściwym *URL* o składni ===`ssh://yourserver.yourcompany.com/home/youruser`===.



Rys. 4. *Micro Focus iManager* – współdzielone katalogi w zainstalowanej usłudze *NetStorage.*

>> TWORZENIE OBIEKTU TYPU STORAGE LOCATION OBJECT

1. Uruchamiamy przeglądarkę internetową – wpisujemy właściwy adres *URL* ===*http://server_ip_address/nps/imanager.html*=== w celu uruchomienia *web*owego programu *iManager*.
2. Po zalogowaniu się do serwera *OES* w lewej kolumnie klikamy ikonę <<*File Access*>>, a następnie ikonę <<*New Storage Location*>>.
3. Wypełniamy pola informacyjne (%%rys. 5%%):



Rys. 5. Tworzenie obiektu w *Micro Focus iManager* – nowe położenie składowania danych.

- nazwa obiektu (*object name*) – nazwa w drzewie katalogowym *eDirectory;*
- nazwa wyświetlana (*display name*) – nazwa obiektu wyświetlana w katalogowej liście dostępowej *NetStorage;*
- położenie katalogu (*directory location*) – lokalizacja katalogu w systemie plików, w postaci *URL*, który zawiera typ systemu plików, nazwę serwera, *volumin* oraz ścieżkę do katalogu; właściwa składnia *URL*, w zależności typu serwera, ma jedną z poniższych postaci:

  a) w przypadku serwera *NetWare*, z systemem plików *NFS* lub *NSS*:
  ===ncp`://server_name/volume/path_to_directory===,`

  b) w przypadku serwera *Linux*: ***===ncp****://server_name/volume/path_to_directory===,*

  c) w przypadku używanych systemów typu *CIFS* lub *Samba*:
  ===cifs*://server_name/cifs_share_name===,*

  d) w przypadku systemów *linu*ksowych, które nie wspierają protokołu *NCP* ani *CIFS*:
  ===ssh*://yourserver.yourcompany.com/home/youruser===;*

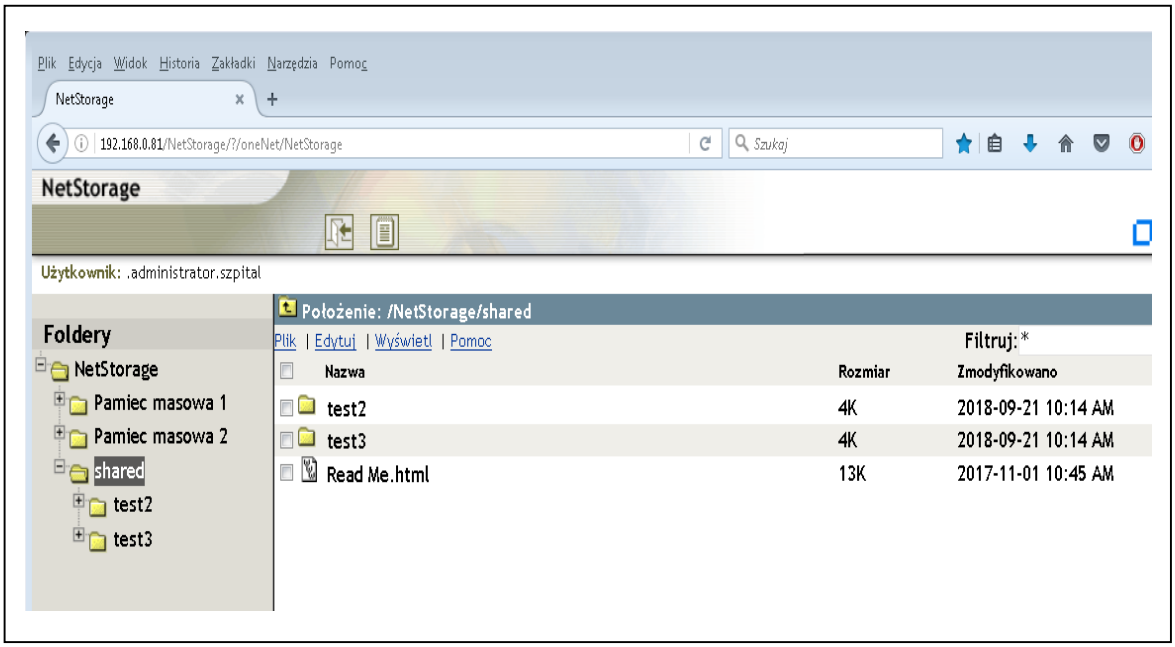
- kontekst (*context*) – kontekst tworzonego obiektu w drzewie katalogowym *eDirectory;*
- komentarz (*comment*) – wprowadzany przez administratora, nie jest jednak wyświetlany.

>> TWORZENIE LISTY TYPU STORAGE LOCATION LIST

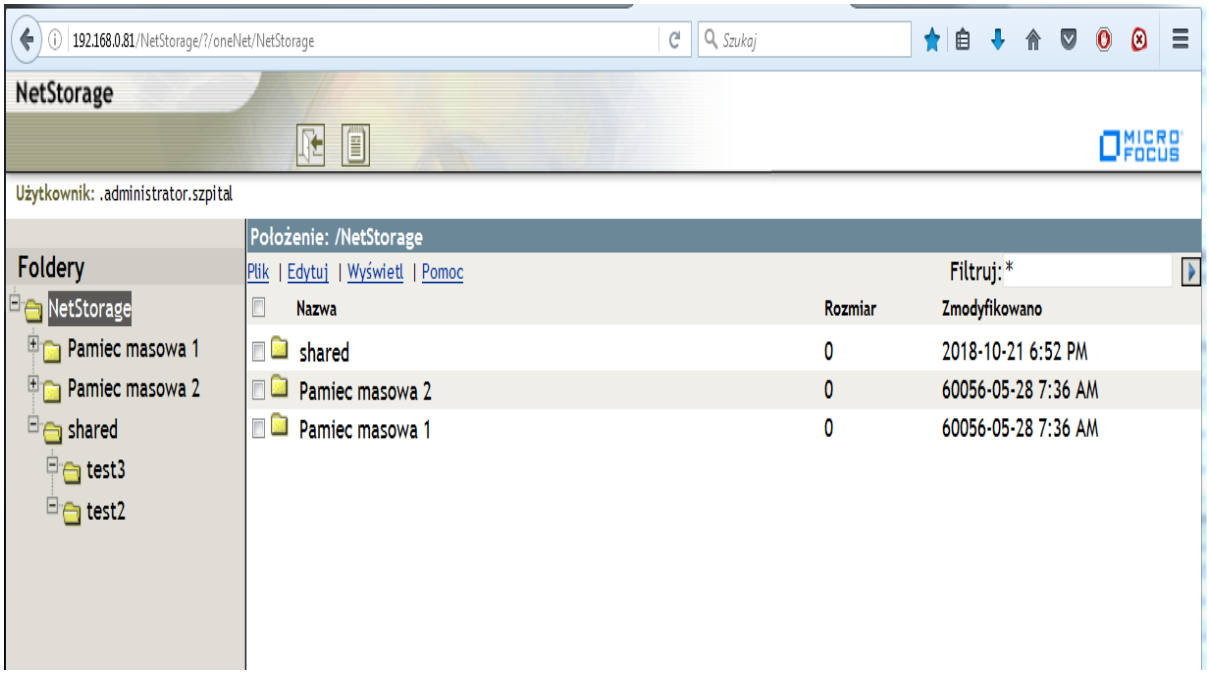
Po utworzeniu obiektu typu *Storage Location Object* administrator musi utworzyć listę obiektów, które mogą być wykorzystane przez określonego użytkownika, tj. grupę, profil lub obiekt kontenerowy. Przy następnym logowaniu użytkownicy mogą zobaczyć foldery powiązane z tą listą obiektów. Może ona być zmieniana – rozszerzana lub skracana. W celu jej utworzenia postępujemy podobnie jak w poprzedniej części.

1. Poprzez przeglądarkę internetową uruchamiamy program *iManager*.
2. Po zalogowaniu się klikamy w lewej kolumnie ikonę <<*File Access*>>, a następnie ikonę <<*Assign Storage Location*>> przyporządkowującą folder magazynowy do obiektu.
3. Klikamy klawisz <<*Object Selector*>> i wybieramy obiekty typu *User*, *Group*, *Profile* lub *Container*, za pomocą których tworzona będzie lista obiektów.
4. Klikamy klawisz <<*Object Selector*>> i wybieramy obiekty typu *Storage Location*, które zamierzamy dołączyć do listy obiektów.

Z chwilą utworzenia i skonfigurowania obiektu typu *Storage Location Object* możliwy jest dostęp – z poziomu *iManager* – do folderów i plików zlokalizowanych na serwerach *netware*'owych i *linux*owych w sieci *LAN*, co pokazano na %%rys. 6%%. W końcu usługa *NetStorage* pozwala na dostęp do tych folderów z poziomu przeglądarki internetowej, co widać na %%rys. 7%%.



Rys. 6. *NetStorage* – udostępnione dla użytkownika katalogi i pliki, widziane z poziomu *iManager.*



Rys. 7. *NetStorage* – udostępnione katalogi użytkownika, widziane z poziomu przeglądarki internetowej.

> KORZYŚCI USŁUGI

W niniejszym artykule pokazano praktyczny sposób szybkiej i efektywnej instalacji oraz konfiguracji usługi *Novell NetStorage*, zapewniającej m.in. następujące korzyści:

- pozwala użytkownikom wykonać z poziomu sieci internetowej bezpieczne operacje na swoich plikach: czytanie/zapisywanie, zmiana nazwy, kasowanie, kopiowanie oraz przenoszenie plików pomiędzy stacjami komputerowymi *WAN/LAN* a serwerami znajdującymi się w sieci *LAN*;
- eliminuje konieczność stosowania przez użytkownika oprogramowania klienckiego *VPN* w celu uzyskania dostępu do swoich folderów i plików zlokalizowanych w sieci *LAN*;
- eliminuje konieczność stosowania *e-maili* w celu kopiowania plików pomiędzy komputerem użytkownika zlokalizowanym w sieci *WAN/LAN* a serwerami zlokalizowanymi w sieci *LAN*;
- wspiera internetowe standardy, takie jak *HTTP*, *HTTPS*, *HTML*, *XML*, *WebDAV*.

AUTOR

Autor pracuje jako specjalista ds. wdrożeń, zajmuje się implementacją nowych technologii w infrastrukturze serwerowej. Jest doktorantem, twórcą artykułów naukowych i technicznych publikowanych w czasopismach.