Wieloplatformowy system archiwizacji danych informatycznych

Marian Wrzesień, Łukasz Olejnik, Piotr Ryszawa

Przemysłowy Instytut Automatyki i Pomiarów PIAP

Streszczenie: Zaprezentowano wieloplatformowy system archiwizacji danych informatycznych w organizacji wyposażonej w sieć informatyczną. Istotą i celem niniejszego rozwiązania jest zapewnienie bezpieczeństwa danych komputerowych, które są przetwarzane w takich systemach operacyjnych jak Linux, Windows, NetWare, z wykorzystaniem zintegrowanego systemu archiwizacji, który komunikuje się z powyższymi OS. Współpracujące z tymi systemami (serwerami) komputery są zarówno stacjonarne, jak i mobilne. Komputery mobilne zostały wyposażone w narzędzia umożliwiające użytkownikowi synchronizację tych komputerów z serwerem archiwizującym. Synchronizacja następuje samoczynnie po dołączeniu ich do sieci informatycznej, po uprzedniej pracy zdalnej. Podczas archiwizowania jest stosowana zasada, że w systemie informatycznym serwerowi archiwizującemu organizacji zapewniono dostęp o najwyższych uprawnieniach do pełnych danych informatycznych. W celu umożliwienia właściwego pobierania danych przez serwer archiwizujący, wszystkie systemy OS są wyposażone w narzędzia, które umożliwiają autoryzowany, jednokierunkowy dostęp do ich systemów poprzez ten serwer. Ze względów bezpieczeństwa, podczas pobierania danych, jak również podczas komunikacji z innymi systemami OS, połączenia serwera archiwizującego z innymi systemami powinny być szyfrowane.

Słowa kluczowe: archiwizacja, synchronizacja, SQL, rsync, rsnapshot

1. Wprowadzenie

Wieloplatformowy system archiwizacji dedykowany jest przechowywaniu danych informatycznych (DI) obejmujących: zarządzanie organizacją - dane księgowe i dane działu wspomagania badań, kontrolę pracowników - obecność (KD) i rejestracja czasu pracy (RCP), komputerowe wspomaganie projektowania (CAD), witryny internetowe obejmujące tak działania marketingowe, jak i wspomaganie realizacji projektów, witryny intranetowe – komunikujące wewnętrznie pracowników organizacji, oraz - posadowione na laptopach - rozproszone dane, powstające podczas pracy w lokalizacjach poza siedzibą firmy.

Ze względu na różną funkcjonalność, wymienione powyżej DI przetwarzane są w odmiennych systemach operacyjnych OS, takich jak: Windows Serwer, Windows Workstation, Linux Serwer, NetWare Serwer. Wspólny dla firmy serwer archiwizujący (SA) posiada zdolność do komunikowania się z tymi systemami OS oraz ma zapewniony dostęp do pobierania określonych DI, w celu ich przechowania.

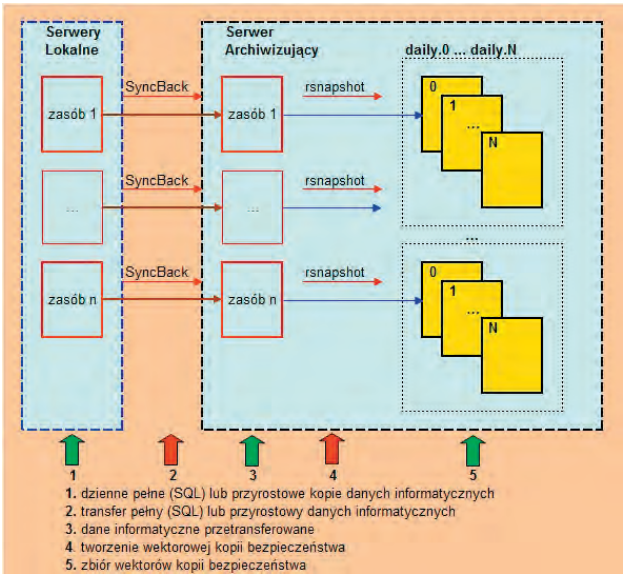
2. System archiwizacji

2.1. Polityka archiwizacji

Polityka archiwizacji określa:

- Dane informatyczne objęte archiwizacją;
- Metodę archiwizacji;
- Termin i cykl archiwizacji;
- Nośnik oraz oprogramowanie służące do archiwizacji;
- Czas i sposób przechowywania archiwów;

W PIAP archiwizowane są - szczegółowo omówione dalej - wymienione we wprowadzeniu dane informatyczne.



Rys. 1. Wektorowy system archiwizacji
Fig.1. The vector system for archiwing

Jako metodę zastosowano archiwizację wektorową [1]. Metoda ta polega na tworzeniu wektora kolejnych, dziennych kopii bezpieczeństwa. Proces ten przebiega w trzech etapach:

- lokalne przygotowanie dziennych kopii DI do transferu,
- pobranie przez SA danych informatycznych objętych archiwizacją (program rsync),
- uaktualnienie wektora archiwizacji przez dodanie nowej pozycji kopii dziennej i usunięcie najstarszej pozycji tego wektora (program rsnapshot).

Jako nośnik DI zastosowano serwer archiwizujący z zaimplementowanym stabilnym OS Linux CentOS 6.1. Umożliwia on zastosowanie w serwerze ww. oprogramowania narzędziowego. Wyposażenie serwera w macierz dyskową zwiększa pewność działania systemu, a zastosowane

4 niezależne dyski o pojemności 1TB każdy, pracujące w trybie HotSwap umożliwiają odłączanie ich z SA bez przerywania pracy serwera i przechowanie poza nim (np. szafa pancerna), do czasu ich kolejnego użycia określonego harmonogramem korzystania z tych dysków. Wybór OS serwera SA wskazuje, że komunikować się będą ze sobą platformy Linux-Linux, Windows Serwer-Linux, Windows Workstation-Linux, NetWare-Linux.

Przyjęto, że archiwizacja DI będzie przeprowadzana codziennie, nad ranem; czas przechowywania każdego zestawu DI wynosić będzie 30 dni.

2.2. Tworzenie wektora DI programem rsnapshot

Program rsnapshot tworzy wektor, którego elementami są dzienne przyrostowe kopie bezpieczeństwa DI. Wektor ten, to jeden katalog zawierający pełną kopię DI oraz zestaw n katalogów zawierających: ostatnio zmodyfikowane pliki oraz odniesienia (linki twarde) do plików nie modyfikowanych od czasu ostatniej archiwizacji. Dzięki podejściu eliminującemu powielanie nie zmienionych plików, oszczędzany jest znaczny obszar przestrzeni dyskowej. W PIAP przyjęto wektory 30. składnikowe.

2.3. Transfer DI programem rsync

Podstawową cechą programu rsync jest możliwość tworzenie kopii przyrostowej katalogów. Dzięki temu przechowywana jest informacja zarówno o danych bieżących jak i danych, których dalsze przetwarzanie zostało zaniechane. Kopiowanie przyrostowe ogranicza się do plików ostatnio zmodyfikowanych, przez co proces ten zajmuje mniej czasu niż podczas tworzenia pełnej kopi DI. Program rsync jest wykorzystywany do transferu - przygotowanych uprzednio lokalnie DI - przeznaczonych do archiwizacji. Pobranie danych tym programem daje pewność, że w serwerze SA znajdują się dzienne przyrostowe kopie bezpieczeństwa DI - przetwarzane następnie po uruchomieniu odpowiednio skonfigurowanego programu rsnapshot. Działanie programu rsync przebiega w tle, z wykorzystaniem protokołu ssh, bez udziału administratora SA. By to osiągnąć zastosowano demon crond zarządzający harmonogramowanym wykonywaniem poleceń transferu DI oraz zastosowano samoczynną autentykację - przy logowaniu się do archiwizowanych serwerów - bazującą na parze kluczy, prywatnym i publicznym, wygenerowanymi przez program ssh-keygen.

2.4. Lokalne przygotowanie dziennych kopii DI

Przygotowanie danych do transferu w serwerach lokalnych polega na umieszczeniu - w określonej lokalizacji - DI w postaci pliku (SQL) lub katalogu utworzonego jako dzienna kopia przyrostowa. Natomiast umożliwienie pobierania danych przez SA z poszczególnych serwerów sieci informatycznej wymaga zaimplementowania usługi sieciowej ssh na każdym z tych serwerów oraz udostępnienie w nich zasobów przeznaczonych do pobrania przez SA. Lokalne przygotowanie dziennych zasobów DI do transferu stanowi trzon prezentowanego opracowania.

3. Archiwizowane dane informatyczne

3.1. SQL (Simple, XChronos, Project, Enterprise Architect)

W PIAP stosowane są serwery z OS Windows Serwer 2008 (wyposażony w MS SQL 2008) oraz Windows Serwer 2003 (wyposażony w MS SQL 2005). Na bazie MS SQL 2008 zostało zaimplementowane repozytorium oprogramowania Enterprise Architect, służącego do modelowania systemów. Zastosowanie bazy SQL do przechowywania projektów tworzonych przy pomocy tego oprogramowania zapewnia bezpieczną i scentralizowaną archiwizację wyników prac współrealizatorów projektu. Serwer MS SQL 2008 to także bazy oprogramowania MS Project Serwer 2007 oraz witryny SharePoint zainstalowane w tym samym środowisku.

W serwerze MS SQL 2005 natomiast, zaimplementowane są bazy programu księgowego SIMPLE oraz programu XChronos (RCP i KD).

Oba przedstawione wyżej serwery są objęte archiwizacją DI.

Istnieją dwa narzędzia archiwizacji danych w MS SQL Serwer. Są to:

- SQL SMS (program graficzny Server Management Studio),
- SQLCMD (linia poleceń Command Line).

W PIAP zastosowano metodę SQL SMS ze względu na pełny dostęp do narzędzi graficznych. Metoda ta daje możliwość graficznej konfiguracji archiwizacji baz danych. W celu wykonania kopii bezpieczeństwa bazy danych należy zalogować się do serwera MS SQL, wybrać bazę przeznaczoną do archiwizacji oraz wybrać typ wykonywanej kopii bezpieczeństwa: Full (Pełna), Differential (Różnicowa). W PIAP stosuje się typ kopii pełnej ze względu na łatwość odtwarzania po ewentualnym uszkodzeniu bazy danych.

Proces tworzenia kopii bezpieczeństwa można wykonać dla następujących modeli odzyskiwania danych:

- FULL
  Jest to podstawowy model odzyskiwania w środowisku produkcyjnym. Zapewnia on większe bezpieczeństwo danych w przypadku awarii niż model Simple czy Bulk Logged. Polega na kopiowaniu bazy danych oraz jej logów transakcyjnych. Po awarii możliwe jest odzyskanie wszystkich danych pod warunkiem odzyskania bieżącego logu transakcyjnego. Z tego względu dobrą praktyką jest przechowywanie logów transakcyjnych na innym dysku niż pliki z danymi. Dzięki logom transakcyjnym można także odzyskać stan bazy danych z dowolnej chwili.
- BULK_LOGGED
  Powinien być stosowany tylko jako dodatek do modelu FULL. Wszystkie informacje potrzebne do odzyskania zwykłych transakcji są archiwizowane tak jak w modelu FULL. Różnica występuje dla operacji masowych (bulk operations) polegających na zapisywaniu do bazy dużych ilości informacji jednocześnie. Zmniejsza to objętość pliku z logami, ale uniemożliwia odtworzenie stanu bazy do wybranego punktu

w czasie. Nie jest zatem zalecane przy częstym odtwarzaniu i powrocie do minionych stanów bazy.

- SIMPLE
  W tym modelu kopiowana jest baza danych z pominięciem logów transakcyjnych. Niemożliwy jest zatem powrót do dowolnego stanu bazy w przeszłości, lecz jedynie do stanu odpowiadającego ostatniej archiwizacji. Metoda ta ma uzasadnione stosowanie w przypadkach wykonywania częstych archiwizacji.

Wybór określonego modelu jest poprzedzony sprawdzeniem bieżącego modelu. W tym celu należy wydać polecenie SQL:
SELECT DATABASEPROPERTYEX('NazwaBazy', 'RECOVERY').

W celu zmiany modelu należy wydać polecenie SQL:
alter database NazwaBazy set recovery WybranyModel

W celu automatyzacji procesu archiwizacji należy wykorzystać narzędzia Maintenance Plan Wizard lub Maintenance Plan Designer.

Maintenance Plan Wizard to kreator prowadzący użytkownika krok po kroku przez proces tworzenia w sposób uproszczony planu konserwacji.

Maintenance Plan Designer natomiast, to interfejs graficzny bazujący na metodzie „przeciągnij i upuść", dostępny w SQL Server Management Studio, pozwalający na bardzo rozbudowane, indywidualne tworzenie planów konserwacji.

Odmienną do opisanej metodą jest SQLCMD.

Archiwizacja przy użyciu SQLCMD wymagałaby stworzenia dwóch skryptów: skrypt.sql oraz skrypt.bat.

Skrypt skrypt.sql zawiera polecenia archiwizacji w formacie SQL. Archiwizacja może być dwojaka: z możliwością wyboru opcji zapisu danych w jednym pliku (kopie baz z wielu dni) lub wielu plikach (każda kopia dzienna w oddzielnym pliku). Przykładowa postać pliku skrypt.sql:

- Dla opcji wszystkie kopie bazy w jednym pliku
  BACKUP DATABASE [NazwaBazy] TO DISK = 'C:\backup\kopia.bak' WITH NOINIT, STATS = 10
  GO;
- Dla opcji każda kopia bazy w oddzielnym pliku
  BACKUP DATABASE [NazwaBazy] TO DISK = 'C:\backup\kopia.bak' WITH INIT, STATS = 10
  GO.

Skrypt skrypt.bat wywołuje połączenie z serwerem MS SQL oraz inicjuje wykonanie poleceń archiwizacji zawartych w pliku skrypt.sql. Poniżej znajduje się przykładowa zawartość pliku skrypt.bat:
sqlcmd -S KOMPUTER\NAZWASERWERASQL -U sa -P "hasło" -i c:\skrypty\skrypt.sql.

Zalecaną metodą archiwizacji baz danych jest ta, która polega na tworzeniu oddzielnego pliku dla każdej kopii dziennej. Ma to istotne znaczenie przy odtwarzaniu baz z zachowaniem ich właściwej kolejności. SQLCMD daje także możliwość odtworzenia bazy danych. Poniżej przedstawiona jest składnia polecenia służącego do odtworzenia bazy:
sqlcmd -S KOMPUTER\ NAZWASERWERSAQL -U sa -P "hasło" -Q "RESTORE DATABASE [NazwaBazy] FROM DISK = 'C:\backup\kopia.bak' WITH FILE = 1, KEEP_REPLICATION, NOUNLOAD, REPLACE, STATS = 10".

Niezależnie od zastosowanej metody archiwizacji lokalnej baz danych, są one pobierane przez serwer SA przy pomocy programu rsync za pośrednictwem połączenia szyfrowanego.

Domyślnie systemy Windows nie zawierają pakietu rsync. W celu umożliwienia połączeń SA przez rsync z systemami Windows należy zainstalować oprogramowanie CopSSH.

CopSSH jest wdrożeniem serwera i klienta SSH dla systemów Windows. Oprogramowanie to nie zawiera domyślnie programu rsync. Program ten należy pobrać z repozytoriów Cygwina i umieścić w katalogu bin CopSSH.
W systemie operacyjnym Windows należy utworzyć użytkownika, który będzie miał uprawnienia do katalogów objętych archiwizacją. Użytkownik ten musi być także aktywowany w oprogramowaniu CopSSH. Hasło aktywowanego użytkownika musi być zgodne z hasłem jakie jest założone w systemie operacyjnym. W celu zapewnienia bezpiecznej komunikacji należy wykorzystać mechanizm dystrybucji kluczy SSH. Klucz publiczny użytkownika serwera archiwizującego należy umieścić w pliku authorized_keys utworzonego użytkownika systemu Windows.

3.2. DMS

System DMS zbudowany jest na oprogramowaniu OpenKM [3]. Jest on posadowiony w serwerze Windows Serwer 2003. Tak jak inne wymienione wyżej zasoby podlega on archiwizacji. Tworzenie kopii bezpieczeństwa polega na archiwizacji katalogu zawierającego repozytorium: $JBOSS_HOME/repository – określonego parametrem repository.home w pliku konfiguracyjnym OpenKM.cfg. Ze względu na istotność zawartych informacji zaleca się również tworzenie kopii bezpieczeństwa plików z katalogu $JBOSS_HOME/ server/default/data/hypersonic. Zawiera on dane:

- OKMActivity: Dziennik aktywności użytkownika - wszystkie działania wykonywane przez użytkownika w DMS.
- OKMAuth: Informacje o użytkownikach, rolach i hasłach.
- OKMWorkflow: Definicje procesów i dane instancji procesu.

Przed rozpoczęciem tworzenia kopii bezpieczeństwa zaleca się zatrzymanie serwera JBoss w celu zapobieżenia modyfikacjom plików w trakcie procesu archiwizacji.

Poniżej przedstawiono przykładowy skrypt służący do tworzenia kopii bezpieczeństwa:
c:\jboss\bin\shutdown.bat -S
xcopy c:\jboss-4.2.3.GA*.* e:\Backup\ /s/e
c:\jboss-4.2.3.GA\bin\run.bat -b 0.0.0.0

Proces tworzenia kopii bezpieczeństwa jest zautomatyzowany przez wykorzystanie Harmonogramu Zadań systemu Windows.

Po wykonaniu, kopia bezpieczeństwa jest kompresowana przez oprogramowanie WinRar, tworząc zasób przygotowany do pobrania przez serwer SA, podobnie jak ma to miejsce w przypadku baz danych MS SQL.

3.3. Stacje mobilne

W celu zapewnienia bezpieczeństwa danych informatycznych pracowników korzystających ze stacji mobilnych opracowano mechanizm archiwizacji kluczowych danych zawartych na tych stacjach. Do takich danych zalicza się przede wszystkim poczta elektroniczna oraz opracowywane dokumenty.

W celu prowadzania archiwizacji, na stacjach mobilnych zastosowano oprogramowanie. Przeznaczone jest ono do użytku osobistego i komercyjnego. Chroni ważne DI, tworząc automatycznie ich kopie zapasowe w folderze, który może znajdować się na urządzeniu USB/Firewire, na dysku lokalnym lub w zasobach sieciowych. Archiwizowane dane można skompresować (przy użyciu standardowego formatu ZIP) lub zapisać jako dokładną kopię pierwotnych plików. Zaletą oprogramowania FBackup jest możliwość archiwizacji otwartych plików. Niezależnie czy w czasie archiwizacji plik jest używany przez inny program, FBackup może zarchiwować ten plik dzięki wykorzystaniu usługi kopiowania woluminów w tle dostępnej w systemie Windows stacji mobilnej. W programie FBackup określa się profil archiwizacji zawierający wszystkie archiwizowane zasoby. Pliki i katalogi stacji mobilnych są synchronizowane z serwerem Windows Server 2008. W serwerze tym zostali utworzeni użytkownicy, których stacje mobilne zostały objęte archiwizacją oraz założono katalogi o strukturach odpowiadających strukturom katalogów stacji mobilnych.

Dane z serwera Windows Serwer 2008 są pobierane przez serwer SA przy użyciu rsync w ramach procesu archiwizacji DI PIAP.

3.4. Autodesk Vault

W obecnych czasach opracowanie złożonych projektów np. robotów czy linii produkcyjnych wymaga współpracy wielu konstruktorów. W PIAP zastosowano w serwerze Windows Serwer 2008 narzędzie wspomagające prace projektowe - Autodesk Vault. Oprogramowanie to pozwala na współpracę grup projektantów oraz wymianę dokumentacji tworzonych opracowań. Pełna integracja z innymi pakietami projektowymi firmy Autodesk stosowanymi w Instytucie, jak AutoCAD czy Autodesk Inventor Professional pozwala na scentralizowane zarządzanie procesem powstawania dokumentacji technicznej projektów. Autodesk Vault to aplikacja działająca na zasadzie klient-serwer, wykorzystująca repozytoria plików tworzonych przez realizatorów projektów oraz bazy danych rejestrujące modyfikacje tych plików. Pliki znajdują się w jedny*m* centralnym magazynie serwera, a bazy danych są przechowywane w MS SQL. Członkowie projektu współdzielą zasoby, mając zawsze dostęp do najnowszej wersji DI wraz z historią ich zmian. Aplikacja Autodesk Vault działa w oparciu o usługi serwer Microsoft IIS (Internet Information Services) w wersji 7.0 oraz bazę danych MS SQL, pracującą w osobnej instancji MS SQL Server 2008. Stacje użytkowników korzystają z klienta Vault zainstalowanego na różnych systemach z rodziny MS Windows m.in. Windows XP, Windows Vista, Windows 7 (32 i 64 bit). Ze względu na brak zautomatyzowanego procesu tworzenia kopii bezpieczeństwa programu Autodesk Vault, w PIAP opracowano taki proces. Podstawowymi zasobami objętymi archiwizacją są wyżej wymienione baza danych oraz repozytoria plików. Do stworzenia lokalnej kopii bezpieczeństwa wymienionych zasobów zastosowano narzędzie wbudowane w MS SQL 2008 – SQL Server Management Studio oraz program WinRar pakujący zasoby repozytoriów. W SQL Server Management Studio utworzono Plan Konserwacji (ang. *Maintenance Plan*) umożliwiający zautomatyzowanie operacji na bazie danych, takich jak: sprawdzenie integralności danych, zmniejszenie rozmiaru poprzez usunięcie pustej przestrzeni, reorganizacja i przebudowanie indeksu, aktualizacja statystyk, pełny backup baz danych, backup logów transakcyjnych oraz prace oczyszczające. Lokalny backup baz danych zapisywany jest w określonym folderze na dysku lokalnym serwera– zgodnie z przedstawioną wyżej polityką archiwizacji.

Archiwizacja wykonywania kopii bezpieczeństwa plików znajdujących się w repozytorium serwera Vault została zautomatyzowana dzięki usłudze Harmonogram Zadań systemu Windows oraz zastosowaniu skryptu typu *.bat:

```
"c:\program files\winrar\rar.exe" a e:\vaultback\repo.rar -
agYYYYMMD -r  E:\REPOZYTORIA\*.*
forfiles -pE:\vaultback\ -m*.rar -d-30 -c"cmd /c del
@FILE"
```

Opracowany skrypt tworzy archiwum typu rar z całą zawartością repozytorium oraz usuwa archiwalne pliki kopii bezpieczeństwa. Skrypt ten jest wykonywany automatycznie przez Harmonogram Zadań Windows. W pierwszym kroku program Winrar, wywoływany przez skrypt, tworzy archiwum o nawie repo.rar Zastosowany parametr –agYYYYMMD skutkuje modyfikacją nazwy archiwum do postaci repoYYYYMMD.rar, gdzie YYYY to bieżący rok, MM to miesiąc, a D to dzień miesiąca. Parametr –r dodaje rekursywnie do archiwum wszystkie podkatalogi repozytorium. W drugim kroku program forfiles przeszukuje folder z utworzonymi wcześniej archiwami *.rar w celu usunięcia zdezaktualizowanych.

Wynikiem opisanych powyżej procesów jest utworzenie lokalnej kopii bezpieczeństwa DI programu Autodesk Vault. Tak przygotowana lokalna kopia bezpieczeństwa pobierana jest przez serwer SA przy użyciu rsync w ramach procesu archiwizacji DI PIAP.

3.5. Witryny Internetowe

Witryny internetowe składają się zwykle z katalogów o strukturze wypełnionej plikami źródłowymi oraz dedykowanych bazy danych, które w PIAP korzystają z serwera MySQL. Ze względu na wielość witryn internetowych i dostęp wielu projektantów do tych witryn, dla zachowania bezpieczeństwa zaimplementowano 4 instancje mysqld [2]. Proces lokalnego przygotowania DI obejmuje utworzenie przyrostowych kopii bezpieczeństwa: użytkowników MySQL oraz baz danych MySQL dla każdej z instancji mysqld oraz katalogów witryn. Wykonywanie kopii bez-

pieczeństwa użytkowników realizuje się z zastosowaniem skryptów mysqldumpgrants udostępnianych przez Free Software Foundation w ramach GNU General Public License. W wyniku ich działania otrzymuje się pliki users.sql dla każdej instancji mysqld. Kopie bezpieczeństwa baz danych wykonywane są z wykorzystaniem skryptu:
mysqldump –u root –phasło -- triggers -- databases Nazwa > arch.sql, gdzie arch.sql jest zarchiwizowaną bazą Nazwa.
Lokalne dzienne zasoby poszczególnych witryn internetowych tworzone są jako przyrostowe kopie bezpieczeństwa wwwX.
Tak więc w procesie przygotowania dziennych kopii bezpieczeństwa, dla N instancji i K baz danych(witryn) w każdej z nich otrzymuje się pliki: users0.sql,...usersN.sql, arch00.sql,...archN0.sql, ... arch0K.sql,...archNK.sql oraz www0,...wwwK*N katalogów witryn.
Ewentualne odtworzenie zarchiwizowanych uprzednio DI wykonuje się za pomocą skryptu:
mysql –u root –phasło –h host –P NrPortu < arch.sql.

3.6. NetWare (pliki)

Serwer Novellowy z zaimplementowanym OS NetWare 6.5 istotnie wspiera pracę zespołową realizatorów projektów oraz grup współpracujących w obszarze wspierania prac naukowo-badawczych. Ze względu na swoje cechy, serwer ten pełni rolę serwera plików, z zasobami zlokalizowanymi w dedykowanych drzewach katalogów, zaprojektowanych pierwotnie dla każdej grupy użytkowników. Taka funkcjonalność powoduje, że każdy chwilowy stan katalogów w tym serwerze stanowi zestaw gotowy do przetworzenia go przez SA. Program rsync dokonuje transferu DI do SA modyfikując przyrostowo katalogi znajdujące się w tym serwerze SA, a program rsnapshot modyfikuje wektor archiwizacji, przetwarzając najnowsze zmodyfikowane katalogi zawierające DI podlegające archiwizacji. W przypadku opisanego procesu archiwizacji, ewentualne odtworzenie przechowywanych DI sprowadza się do pobrania z SA kopii poszukiwanego pliku.
Realizacja przedstawionego procesu archiwizacji wymagała zaimplementowania w serwerze NetWare serwera ssh, zapewniającego warunki szyfrowanego transferu DI.

Bibliografia

1. Marian Wrzesień, *Wektorowa archiwizacja danych wykorzystująca przyrostowe kopie bezpieczeństwa*. PAR, 2009, s.240-248.
2. Marian Wrzesień; Piotr Ryszawa, *Multi-instancyjny, wielowątkowy system bazodanowy MySQL, w środowisku OS Fedora kontrolowanym przez SELinux*. PAR, 2011, s..315-322.
3. Marian Wrzesień; Piotr Ryszawa, *System zarządzania dokumentami projektu Proteus zaimplementowany w OpenKM*. PAR, 2010, s. 217-227..
4. W. Curtis Preston, Archiwizowanie i odzyskiwanie danych, Helion SA, 2008.
5. Simson Garfinkel, Gene Spafford, UNIX and Internet Security, Second Edition O'Reilly MediaPractical, 1996.

The multi-platform computer data backup system

Abstract: The multi-platform computer data backup system in an organization equipped with a computer network is presented. The essence and purpose of this arrangement is to ensure the security of computer data which are processed in such operating systems as Linux, Windows, NetWare, using an integrated archiving system which communicates with the above OS systems Compatible with these systems (servers) computers are both stationary and mobile. Mobile computers are equipped with tools that enable users to synchronize those PCs to the server archiving. Synchronization occurs when you attach them to the computer network, after first working remotely. While archiving is applied the principle that in the organization computer system, archiving server has access to all computer data with the highest privileges. In order to allow proper collection of data by the archive server, all OS systems are equipped with tools that enable authorized, one-way access to the systems in the organization through this server. For security reasons, when retrieving data, as well as when communicating with other OS systems, archiving server connection to other systems should be encrypted.

Keywords: archiving, synchronization, SQL, rsync, rsnapshot

dr. inż. Marian Wrzesień
Główny Informatyk Instytutu, Administrator Sieci Informatycznej PIAP-LAN, Adiunkt
e-mail: mwrzesien@piap.pl

mgr. inż. Łukasz Olejnik
Inżynier sprzętowy Sieci Informatycznej PIAP-LAN,
e-mail: lolejnik@piap.pl

inż. Piotr Ryszawa
Programista Sieci Informatycznej PIAP-LAN,
e-mail: pryszawa@piap.pl