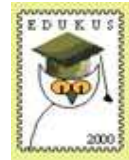




„Pracownia internetowa w każdej szkole” (edycja Jesień 2007)



Opiekun pracowni internetowej cz. 2 (D2) ISA Server - Logi serwera

Zadanie 5 Sprawdzanie logów serwera



Notatka – logi na serwerze SBS 2003

W wersji Jesień 2007 serwera SBS2003 R2 wszystkie logi znajdują się na serwerze w lokalizacji
`O:\log\isa2004`

lub w udziale sieciowym

`\\nazwa_serwera\o$\log\isa2004`

`%logonserver%\o$\log\isa2004`

Co znajduje się w logach gromadzonych na serwerze SBS 2003

zawierają szczegółowe informacje na temat ruchu pomiędzy siecią lokalną i Internetem (m.in. nazwa użytkownika, adres stacji, adres komputera docelowego, nr portu oraz nazwę programu, który korzystał z Internetu)

.....
.....

zawierają szczegółowe informacje na temat stron internetowych oglądanych przez użytkowników (m.in. nazwa użytkownika, adres stacji, adres komputera docelowego, nr portu oraz nazwę programu, który korzystał z sieci WEB, nazwy plików pobranych z Internetu)

.....
.....

zawierają szczegółowe informacje na temat ruchu w sieci pod kątem reguł i filtrów ustalonych przez administratora

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

**Polecenie 1 – Podgląd zdarzeń w czasie rzeczywistym**

1. Wybierz z paska zadań **Start** ⇒ **Wszystkie programy** ⇒ **Microsoft ISA Server** ⇒ **ISA Management**
2. Rozwiń **swój serwer**
3. Wskaż **Monitoring**
4. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wyszukaj zakładkę **Logging**
5. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wskaż zakładkę **Logging**
6. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz zakładkę **Tasks**
7. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz opcję **Edit Filter**
8. W oknie **Edit Filter** wskaż z listy **Log Record Type**
9. Zauważ że przycisk **Update** jest nieaktywny
10. W oknie **Edit Filter** z listy rozwijanej **Value** wybierz **Firewall**
11. W oknie **Edit Filter** wybierz przycisk **Update**
12. W oknie **Edit Filter** z listy rozwijanej **Value** wybierz **Firewall or Web Proxy Filter**
13. W oknie **Edit Filter** wybierz przycisk **Update**
14. W oknie **Edit Filter** wskaż z listy **Log Time**
15. W oknie **Edit Filter** z listy rozwijanej **Condition** wybierz **Last 24 Hours**
16. W oknie **Edit Filter** wybierz przycisk **Update**
17. W oknie **Edit Filter** z listy rozwijanej **Condition** wybierz **Live**
18. W oknie **Edit Filter** wybierz przycisk **Update**
19. Upewnij się czy w oknie **Edit Filter** na liście filtrów znajdują się tylko dwa filtry:
Log Record Type oraz **Log Time**
20. Jeżeli w oknie **Edit Filter** znajdują się dwa powyższe filtry wybierz przycisk **Start Query**, w innym przypadku usuń pozostałe filtry zaznaczając je i używając przycisku **Remove**
21. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wyświetlane są na bieżąco wszelkie informacje dotyczące sieci
22. Nie zamykaj okna **Microsoft Internet Security and Acceleration Server 2004**
23. Uruchom wiersz poleceń wybierając z paska zadań serwera **Start** -> **Wiersz polecenia**
24. W oknie wiersza poleceń wpisz polecenie **ping www.sejm.gov.pl** i naciśnij klawisz **enter**
25. Zamknij okno wiersza poleceń
26. Jakie informacje widzisz w oknie **Microsoft Internet Security and Acceleration Server 2004**?
.....
.....
.....
27. Zamknij okno **Microsoft Internet Security and Acceleration Server 2004**

**Polecenie 2 – Definiowanie dodatkowych kolumn w podglądzie zdarzeń**

1. Wybierz z paska zadań **Start** ⇒ **Wszystkie programy** ⇒ **Microsoft ISA Server** ⇒ **ISA Management**
2. Rozwiń **swój serwer**
3. Wskaż **Monitoring**
4. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wyszukaj zakładkę **Logging**
5. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wskaż zakładkę **Logging**
6. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz zakładkę **Tasks**
7. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz opcję **Start Query**
8. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz prawym przyciskiem myszy wiersz tytułowy dolnej ramki, w której wyświetlane są zdarzenia sieciowe
9. Wybierz z menu podręcznego **Add/Remove Columns...**
10. W oknie **Add/Remove Columns** wybierz **Client Agent** z kolumny **Available columns**
11. W oknie **Add/Remove Columns** wybierz przycisk **Add->**
12. W oknie **Add/Remove Columns** przy pomocy przycisku **MoveUp** ustaw **Client Agent** w pierwszym wierszu
13. W oknie **Add/Remove Columns** przy pomocy przycisku **MoveUp/Down** ustaw **Client Username** w drugim wierszu
14. W oknie **Add/Remove Columns** wybierz przycisk **OK**
15. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** kolumny zdarzeń zostały wyświetlone w innej kolejności
-
-
-
28. Zamknij okno **Microsoft Internet Security and Acceleration Server 2004**

**Notatka –**

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....



1

Polecenie 3 – Podgląd wcześniejszych zdarzeń, ograniczonych do konkretnych kont

1. Zaloguj się na stacji roboczej jako administrator i zainstaluj z płyty szkoleniowej program Gadu Gadu
2. Wyloguj się i zaloguj się jako *nauczyciel0xxn*
3. Uruchom program Gadu Gadu
4. W programie Gadu Gadu załóż nowe konto:

Zapisz numer swoje konta Gadu Gadu:

Zapisz hasło do swojego konta Gadu Gadu:

Zapisz numery kont Gadu Gadu swoich sąsiadów:

5. W programie Gadu Gadu dodaj do listy kontaktów swoich sąsiadów i wymień z nimi grzecznościowe informacje:
6. Zaloguj się na konsoli serwera jako administrator
7. Wybierz z paska zadań
Start ⇒ Wszystkie programy ⇒ Microsoft ISA Server ⇒ ISA Management
8. Rozwiń **swój serwer**
9. Wskaż **Monitoring**
10. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wyszukaj zakładkę **Logging**
11. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wskaż zakładkę **Logging**
12. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz zakładkę **Tasks**
13. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz opcję **Edit Filter**
14. W oknie **Edit Filter** wskaż z listy **Log Time**
15. W oknie **Edit Filter** z listy rozwijanej **Condition** wybierz **Last 24 hours**
16. W oknie **Edit Filter** wybierz przycisk **Update**
17. W oknie **Edit Filter** z listy **Filter by** wybierz **Client Username**
18. W oknie **Edit Filter** z listy **Condition** wybierz **Contains**
19. W oknie **Edit Filter** w polu **Value** wpisz **nauczyciel**
20. W oknie **Edit Filter** wybierz przycisk **Add To list**
21. W oknie **Edit Filter** wybierz przycisk **Start query**
22. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wyświetlane zostały wszelkie informacje dotyczące kont posiadających w nazwie **nauczyciel** i korzystających z sieci Internet

**Notatka –**

.....

.....

.....

.....

.....

**Polecenie 4 – Podgląd wcześniejszych zdarzeń, ograniczonych do konkretnych kont i aplikacji**

1. Wybierz z paska zadań **Start** ⇒ **Wszystkie programy** ⇒ **Microsoft ISA Server** ⇒ **ISA Management**
2. Rozwiń **swój serwer**
3. Wskaż **Monitoring**
4. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wyszukaj zakładkę **Logging**
5. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wskaż zakładkę **Logging**
6. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz zakładkę **Tasks**
7. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz opcję **Edit Filter**
8. W oknie **Edit Filter** wskaż z listy **Log Time**
9. W oknie **Edit Filter** z listy rozwijanej **Condition** wybierz **Last 24 hours**
10. W oknie **Edit Filter** wybierz przycisk **Update**
11. W oknie **Edit Filter** z listy **Filter by** wybierz **Client agent**
12. W oknie **Edit Filter** z listy **Condition** wybierz **Contains**
13. W oknie **Edit Filter** w polu **Value** wpisz **gg**
14. W oknie **Edit Filter** wybierz przycisk **Add To list**
15. W oknie **Edit Filter** wybierz przycisk **Start query**
16. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wyświetlane zostały wszelkie informacje dotyczące kont korzystających z aplikacji **gg** posiadających w nazwie **nauczyciel**

**Notatka –**

.....

.....

.....

.....

.....



1

Polecenie 5 – Wykonuje tylko jedna osoba pracująca na konsoli serwera. Określenie przez ile dni przechowywane są logi

1. Wybierz z paska zadań **Start** ⇒ **Wszystkie programy** ⇒ **Microsoft ISA Server** ⇒ **ISA Management**
2. Rozwiń **swój serwer**
3. Wskaż **Monitoring**
4. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wyszukaj zakładkę **Logging**
5. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wskaż zakładkę **Logging**
6. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz zakładkę **Tasks**
7. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz opcję **Configure Firewall Logging**
8. W oknie **Firewall Logging Properties** wybierz przycisk **Options**
9. W oknie **Options** w polu **Delete files older than (days)** wpisz **730** zamiast **365**
10. W oknie **Options** wybierz przycisk **OK**
11. W oknie **Firewall Logging Properties** wybierz przycisk **OK**
12. W oknie **Microsoft Internet Security and Acceleration Server 2004** wybierz przycisk **Apply**
13. W oknie **Apply New Configuration** wybierz przycisk **OK**.
14. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz opcję **Configure Web Proxy Logging**
15. W oknie **Configure Web Proxy Logging** wybierz przycisk **Options**
16. W oknie **Options** w polu **Delete files older than (days)** wpisz **730** zamiast **365**
17. W oknie **Options** wybierz przycisk **OK**
18. W oknie **Configure Web Proxy Logging** wybierz przycisk **OK**
19. W oknie **Microsoft Internet Security and Acceleration Server 2004** wybierz przycisk **Apply**
20. W oknie **Apply New Configuration** wybierz przycisk **OK**.
21. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz opcję **SMTP Message Screener Logging**
22. W oknie **SMTP Message Screener Logging** wybierz przycisk **Options**
23. W oknie **Options** w polu **Delete files older than (days)** wpisz **730** zamiast **365**
24. W oknie **Options** wybierz przycisk **OK**
25. W oknie **SMTP Message Screener Logging** wybierz przycisk **OK**
26. W oknie **Microsoft Internet Security and Acceleration Server 2004** wybierz przycisk **Apply**
27. W oknie **Apply New Configuration** wybierz przycisk **OK**.

**Polecenie 6 – Wykonuje tylko jedna osoba pracująca na konsoli serwera. Sprawdzenie miejsca przechowywanie logów ISA (wykonuje jedna osoba)**

1. Wybierz z paska zadań **Start -> Mój komputer**
2. W oknie **Mój komputer** otwórz dysk **O:**
3. W oknie **O:** otwórz folder o nazwie **LOG**
4. W oknie **O:\LOG** otwórz folder o nazwie **ISA2004**

Zapisz Ile MB zajmują dotychczas zgromadzone logi ISA:

Zapisz ile rodzajów plików zapisuje w logach serwer ISA:

5. Wybierz z paska zadań
Start ⇒ Wszystkie programy ⇒ Microsoft ISA Server ⇒ ISA Management
6. Rozwiń **swój serwer**
7. Wskaż **Monitoring**
8. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wyszukaj zakładkę **Logging**
9. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wskaż zakładkę **Logging**
10. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz zakładkę **Tasks**
11. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz opcję **Configure Firewall Logging**
12. W oknie **Firewall Logging Properties** wybierz przycisk **Options**
13. W oknie **Options** sprawdź co jest wpisane w polu **This folder (enter the full path):**
14. W oknie **Options** wybierz przycisk **Cancel**.
15. W oknie **Firewall Logging Properties** wybierz przycisk **Anuluj**
16. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz opcję **Configure Web Proxy Logging**
17. W oknie **Configure Web Proxy Logging** wybierz przycisk **Options**
18. W oknie **Options** sprawdź co jest wpisane w polu **This folder (enter the full path):**
19. W oknie **Options** wybierz przycisk **Cancel**.
20. W oknie **Configure Web Proxy Logging** wybierz przycisk **Anuluj**
21. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz opcję **SMTP Message Screener Logging**
22. W oknie **SMTP Message Screener Logging** wybierz przycisk **Options**
23. W oknie **Options** sprawdź co jest wpisane w polu **This folder (enter the full path):**
24. W oknie **Options** wybierz przycisk **Cancel**
25. W oknie **SMTP Message Screener Logging** wybierz przycisk **Anuluj**
26. Zamknij okno **Microsoft Internet Security and Acceleration Server 2004**



Polecenie 7 – Analiza logów w Arkuszu Kalkulacyjnym

1. Wybierz z paska zadań **Start** ⇒ **Wszystkie programy** ⇒ **Microsoft ISA Server** ⇒ **ISA Management**
2. Rozwiń **swój serwer**
3. Wskaż **Monitoring**
4. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wyszukaj zakładkę **Logging**
5. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wskaż zakładkę **Logging**
6. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz zakładkę **Tasks**
7. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz opcję **Edit Filter**
8. W oknie **Edit Filter** wskaż z listy **Log Record Type**
9. W oknie **Edit Filter** z listy rozwijanej **Value** wybierz **Firewall or Web Proxy Filter**
10. W oknie **Edit Filter** wybierz przycisk **Update**
11. W oknie **Edit Filter** wskaż z listy **Log Time**
12. W oknie **Edit Filter** z listy rozwijanej **Condition** wybierz **Last Hour**
13. W oknie **Edit Filter** wybierz przycisk **Update**
14. Upewnij się czy w oknie **Edit Filter** na liście filtrów znajdują się tylko dwa filtry:

Log Record Type

Log Time

15. Jeżeli w oknie **Edit Filter** znajdują się tylko te dwa powyższe filtry wybierz przycisk **Start Query**, w innym przypadku usuń pozostałe filtry wskazując je i używając przycisku **Remove**
16. W środkowej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wyświetlane są informacje z ostatniej godziny
17. Poczekaj na wyświetlenie wszystkich informacji
18. W prawej kolumnie okna **Microsoft Internet Security and Acceleration Server 2004** wybierz opcję **Copy All Results to Clipboard**
19. Uruchom arkusz kalkulacyjny **Excel**
20. W oknie Arkusza wybierz z menu **Edycja -> Wklej**
21. W oknie Arkusza wybierz z menu **Dane -> Filtr -> Autofiltr**



Notatka –

.....

.....

.....

.....

.....

.....