

## 3주차 2차시 로그관리

### 【학습목표】

1. 로그 관리의 개념을 설명할 수 있다.
2. 각각 사용하는 로그 관리를 구분할 수 있으며, 응용할 수 있다.

### 학습내용1 : AAA 및 운영체제의 로그 관리

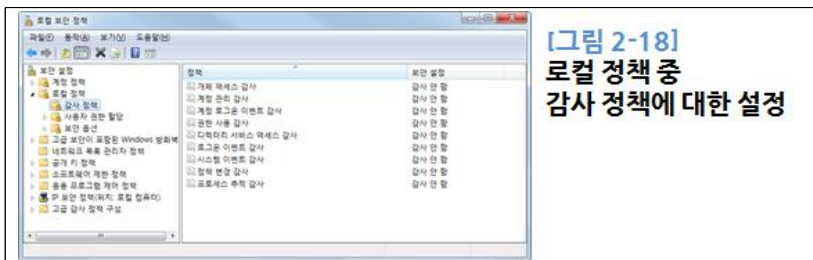
#### 1. AAA

- ① Authentication(인증) : 자신의 신원(Identity)을 시스템에 증명하는 과정으로, 아이디와 패스워드를 입력하는 과정
- ② Authorization(인가) : 올바른 지문을 입력하거나 올바른 패스워드를 입력해 시스템에 로그인인 허락된 사용자라고 판명되어 로그인되는 과정
- ③ Accounting : 시스템에 로그인한 후 시스템이 이에 대한 기록을 남기는 활동

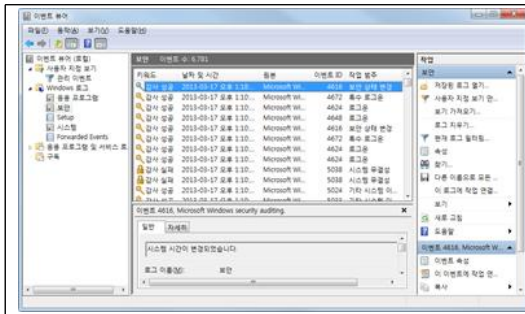
#### 2. 운영체제의 로그 관리

##### 1) 윈도우의 로그

- \* 윈도우의 로그란 : 윈도우는 이벤트(Event)라고 불리는 중앙 집중화된 형태로 로그를 수집하여 저장
- \* 윈도우에서 로깅 항목과 설정 사항 : [제어판]-[관리 도구]-[로컬 보안 정책]의 [로컬 정책]-[감사 정책] 메뉴에서 확인할 수 있음



- 로깅 정책을 적용하면 [제어판]-[관리 도구]-[이벤트 뷰어]를 통해 쌓이는 로깅 정보를 확인할 수 있음



[그림 2-19]  
이벤트 뷰어를 이용한  
보안 로그 확인

[표 2-3] 이벤트 뷰어에 표시되는 내용

항목	설명
종류	성공 감사와 실패 감사가 있으며, 성공 감사는 시도가 성공했을 때, 실패 감사는 어떤 시도가 실패했을 때 남기는 로그임
날짜, 시간	로그를 남긴 날짜와 시간
원본, 범주	로그와 관계 있는 영역
이벤트	윈도우에서는 각 로그별로 고유한 번호를 부여하며, 로그를 분석할 때 이 번호를 알고 있으면 빠르고 효과적인 분석이 가능함
사용자	관련 로그를 발생시킨 사용자
컴퓨터	관련 로그를 발생시킨 시스템

[표 2-4] 윈도우의 로그 종류

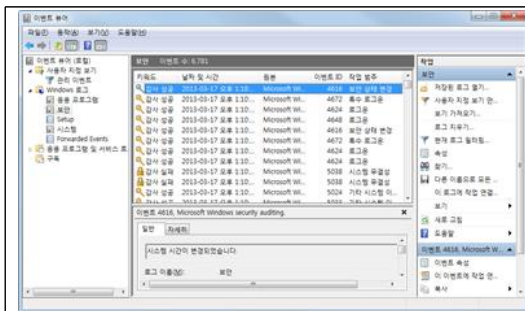
항목	설명
개체 액세스 감사	특정 파일이나 디렉터리, 레지스트리 키, 프린터 등과 같은 객체에 대하여 접근을 시도하거나 속성 변경 등을 탐지함
계정 관리 감사	신규 사용자, 그룹의 추가, 기존 사용자 그룹의 변경, 사용자의 활성화나 비활성화, 계정 패스워드 변경 등을 감사함
계정로그인 이벤트감사	로그온 이벤트 감사와 마찬가지로 계정의 로그인에 대한 사항을 로그로 남기는데 이 둘의 차이점은 전자는 도메인 계정의 사용으로 생성되는 것이며, 후자는 로컬 계정의 사용으로 생성되는 것임
권한 사용 감사	권한 설정 변경이나 관리자 권한이 필요한 작업을 수행할 때 로깅함

[표 2-4] 윈도우의 로그 종류

항목	설명
프로세스 추적 감사	사용자 또는 응용 프로그램이 프로세스를 시작하거나 중지할 때 해당 이벤트가 발생함
시스템 이벤트	시스템의 시동과 종료, 보안 로그 삭제 등 시스템의 주요한 사항에 대한 이벤트를 남김

[표 2-4] 윈도우의 로그 종류

항목	설명
로그인 이벤트 감사	<ul style="list-style-type: none"> <li>로컬 계정의 접근 시 생성되는 이벤트를 감사하는 것임</li> <li>계정 로그인 이벤트 감사에 비해 다양한 종류의 이벤트를 확인할 수 있음</li> </ul>
디렉터리 서비스 액세스 감사	시스템 액세스 제어 목록(SACL)이 지정되어 있는 액티브 디렉터리(Active Directory) 개체에 접근하는 사용자에게 대한 감사 로그를 제공함
정책 변경 감사	사용자 권한 할당 정책, 감사 정책 또는 신뢰 정책의 변경과 관련된 사항을 로깅함



[그림 2-19] 이벤트 뷰어를 이용한 보안 로그 확인

## 2) 유닉스의 로그

\* 리눅스(유닉스) 시스템 : 윈도우와 달리 일반적으로 중앙 집중화되어 관리되지 않고, 분산되어 생성

<b>/usr/adm</b>	(초기 유닉스) HP-UX 9.X, SunOS 4.x
<b>/var/adm</b>	(최근 유닉스) 솔라리스, HP-UX 10.x 이후, IBM AIX
<b>/var/log</b>	FreeBSD, 솔라리스 (/var/adm 와 나누어 저장), 리눅스
<b>/var/run</b>	일부 리눅스

## 3) UTMP

- 유닉스 시스템의 가장 기본적인 로그

- 로그인 계정 이름, 로그인한 환경(initab id), 로그인한 디바이스(console, tty 등), 로그인한 셸의 프로세스 ID, 로그인한 계정의 형식, 로그오프 여부, 시간에 대한 저장 구조(structure)를 확인할 수 있음

- utmp는 텍스트가 아닌 바이너리 형태로 로그가 저장됨

```

root@wishfree:/var/adm
File Edit View Search Terminal Help
[root@wishfree adm]# w
00:49:13 up 1:40, 2 users, load average: 0.24, 0.12, 0.13
USER      TTY      FROM              LOGIN@   IDLE   JCPU   PCPU   WHAT
wishfree  :0              :0        23:09   ?xdm?   56.82s  0.13s  gdm-session-wor
wishfree pts/0      :0        23:10   0.00s   0.20s  1.07s  gnome-terminal
[root@wishfree adm]#

```

**[그림 2-22] w 명령 실행 결과**

#### 4) WTMP

- utmp 데몬과 비슷하게 사용자들의 로그인, 로그아웃, 시스템의 재부팅에 대한 정보를 담고 있음
- last 명령을 이용하여 내용을 확인할 수 있음

```

root@wishfree:/var/adm
File Edit View Search Terminal Help
[root@wishfree adm]# last
reboot      system boot  3.3.7-1.fc17.i68 Wed Jun 6 23:09 - 00:51 (01:42)
wishfree pts/0      :0        Wed Jun 6 23:10 - crash (00:-1)
wishfree :0              :0        Wed Jun 6 23:09 - crash (00:00)
(unknown :0 :0        Wed Jun 6 23:09 - 23:09 (00:00)
reboot      system boot  3.3.7-1.fc17.i68 Wed Jun 6 05:34 - 00:51 (19:17)
wishfree pts/0      :0        Wed Jun 6 05:36 - crash (00:-2)
wishfree :0              :0        Wed Jun 6 05:36 - crash (00:-1)
(unknown :0 :0        Wed Jun 6 05:34 - 05:36 (00:01)
wishfree pts/0      :0        Wed Jun 6 05:33 - 05:36 (00:03)
wishfree pts/0      :0        Wed Jun 6 05:16 - 05:33 (00:16)
wishfree :0              :0        Wed Jun 6 05:15 - 05:34 (00:19)
(unknown :0 :0        Wed Jun 6 05:14 - 05:15 (00:00)
reboot      system boot  3.3.4-5.fc17.i68 Wed Jun 6 04:31 - 00:51 (20:20)

wtmp begins Wed Jun 6 04:31:20 2012
[root@wishfree adm]#

```

**[그림 2-23] last 명령 실행 결과**

#### 5) Secure

- 페도라와 CentOS, 레드햇 등의 리눅스는 secure 파일에 원격지 접속 로그와 su(switch user) 및 사용자 생성 등의 보안과 직접적으로 연관된 로그가 저장됨

```

root@wishfree:/var/log
File Edit View Search Terminal Help
[root@wishfree log]# cat secure
Jun 6 05:14:58 wishfree gdm-welcome[847]: pam_unix(gdm-welcome:session): session opened for user gdm by (uid=0)
Jun 6 05:15:05 wishfree polkitd(authority=local): Registered Authentication Agent for unix-session:2 (system bus name :1.34 [gnome-shell --gdm-mode], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Jun 6 05:15:13 wishfree gdm-password[941]: pam_unix(gdm-password:session): session opened for user wishfree by (unknown)(uid=0)
Jun 6 05:15:13 wishfree gdm-welcome[847]: pam_unix(gdm-welcome:session): session closed for user gdm
Jun 6 05:15:13 wishfree polkitd(authority=local): Unregistered Authentication Agent for unix-session:2 (system bus name :1.34, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Jun 6 05:15:19 wishfree polkitd(authority=local): Registered Authentication Agent for unix-session:3 (system bus name :1.61 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)

```

**[그림 2-24] /var/adm/sulog 파일의 내용**

- 일반 유닉스에서 su 로그는 /var/adm/sulog 파일에 텍스트 형식으로 남음

**[날짜] [시간] [+ (성공) or - (실패)] [터미널 종류] [권한 변경 전 계정 - 변경 후 계정]**

## 6) History

- 명령창에서 실행했던 명령에 대한 기록은 history 명령으로 확인할 수 있음



**history**  
명령 실행 결과

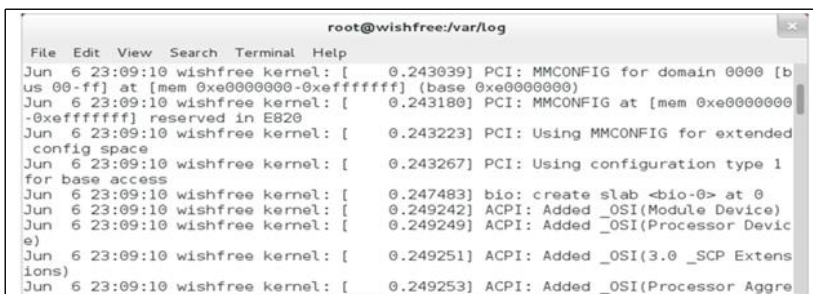
```

root@wishfree:~
File Edit View Search Terminal Help
[root@wishfree ~]# history
 1  ls
 2  yum install httpd
 3  httpd start
 4  ipconfig
 5  ifconfig
 6  /etc/init.d/httpd start
 7  cd /etc
 8  cd init.d
 9  ls
10  yum install httpd
11  ls

```

## 7) Syslog

- 시스템의 운영과 관련한 전반적인 로그
- /var/log/messages 파일에 하드웨어의 구동, 서비스의 동작과 에러 등 다양한 로그를 남김



**[그림 2-26] syslog의 내용**

```

root@wishfree:/var/log
File Edit View Search Terminal Help
Jun  6 23:09:10 wishfree kernel: [ 0.243039] PCI: MMCONFIG for domain 0000 [b
us 00-ff] at [mem 0xe0000000-0xffffffff] (base 0xe0000000)
Jun  6 23:09:10 wishfree kernel: [ 0.243180] PCI: MMCONFIG at [mem 0xe0000000
-0xffffffff] reserved in E820
Jun  6 23:09:10 wishfree kernel: [ 0.243223] PCI: Using MMCONFIG for extended
config space
Jun  6 23:09:10 wishfree kernel: [ 0.243267] PCI: Using configuration type 1
for base access
Jun  6 23:09:10 wishfree kernel: [ 0.247483] bio: create slab <bio-0> at 0
Jun  6 23:09:10 wishfree kernel: [ 0.249242] ACPI: Added _OSI(Module Device)
Jun  6 23:09:10 wishfree kernel: [ 0.249249] ACPI: Added _OSI(Processor Devic
e)
Jun  6 23:09:10 wishfree kernel: [ 0.249251] ACPI: Added _OSI(3.0 _SCP Extens
ions)
Jun  6 23:09:10 wishfree kernel: [ 0.249253] ACPI: Added _OSI(Processor Aggre

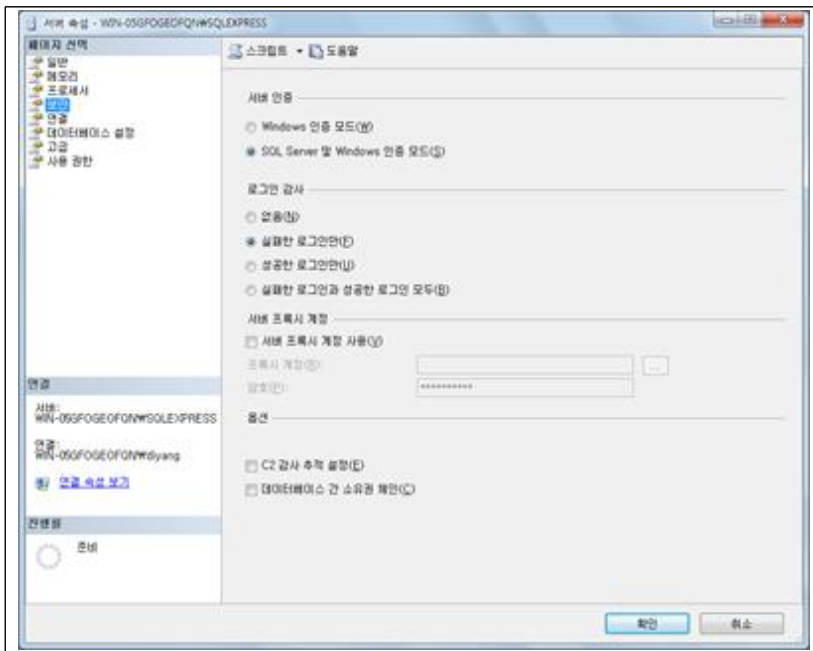
```

## 학습내용2 : 데이터베이스의 로그 관리

## 1. MS-SQL의 로그

- \* MS-SQL : Microsoft SQL Server Management Studio에서 서버를 선택한 뒤, 속성 팝업 창의 [보안] 메뉴에서 일반 '로그인 감사'와 'C2 감사 추적'을 설정할 수 있음

## 1) [그림 2-27] 감사 수준 설정



- C2 감사 추적은 데이터베이스가 생성 · 삭제 · 변경되는지에 대한 자세한 정보를 로그로 남기는 것
- 빈번한 접속이 있는 데이터베이스의 경우 대량의 로그를 생성할 수 있음

## 2. 오라클의 로그

\* 오라클에서 감사 로그를 활성화시키려면 : 먼저 오라클 파라미터파일 (\$ORACLE\_HOME/dbs/init.ora)의 AUDIT\_TRAIL 값을 'DB' 또는 'TRUE' 값으로 지정해야 함

### 1) [그림 2-28] 오라클 감사 로그 설정



### 2) [표 2-5] AUDIT\_TRAIL 설정 값

- AUDIT\_TRAIL 값을 지정한 후에는 '\$ORACLE\_HOME \wrdbs\wadmin \wcataudit.sql'를 실행시킴
- 감사 로그가 활성화된 후 오라클에서 남길 수 있는 데이터베이스 감사의 종류는 문장 감사, 권한 감사, 객체 감사가 있음



AUDIT_TRAIL 값	AUDIT_TRAIL 내용
NONE 또는 FALSE	데이터베이스 감사를 비활성화시킴
DB 또는 TRUE	데이터베이스 감사를 활성화시킴
OS	감사 로그를 OS상의 파일로 저장 이때 경로명은 audit_file_dest에 의해 지정

<b>문장 감사</b>	(Statement Auditing) 지정된 문장을 실행시켰을 경우 기록을 남김
<b>권한 감사</b>	(Privilege Auditing) 특정한 권한을 사용했을 때 기록을 남김
<b>객체 감사</b>	(Object Auditing) 특정한 객체에 대한 작업을 했을 경우 기록을 남김

## 3) [표 2-6] 주요 오라클 감사 뷰

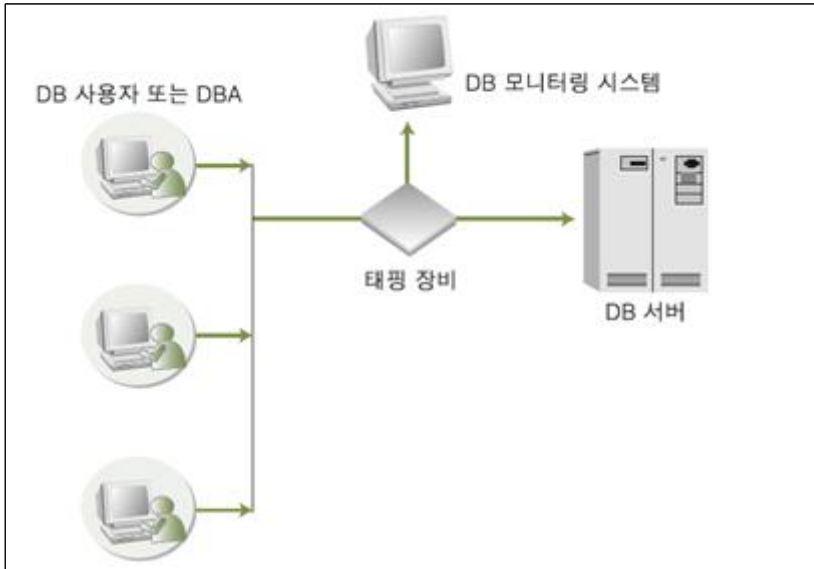
뷰	설명
dba_stmt_audit_opts	문장 감사의 옵션 확인
dba_priv_audit_opts	권한 감사의 옵션 확인
dba_obj_audit_opts	객체 감사의 옵션 확인
dba_audit_trail	데이터베이스의 모든 감사 로그를 출력
dba_audit_object	데이터베이스의 객체와 관련된 모든 감사 로그를 출력

뷰	설명
user_audit_object	현재 사용자의 객체와 관련된 모든 감사 로그를 출력
dba_audit_session	사용자의 로그인 로그오프에 대한 감사 로그를 출력
dba_audit_statement	문장 감사 로그를 출력
dba_audit_object	객체 감사 로그를 출력

### 3. 데이터베이스 모니터링

- 데이터베이스에 대한 로그를 남기는 가장 좋은 방법은 별도의 데이터베이스 모니터링 툴을 도입하는 것
- 네트워크에 네트워크 트래픽을 모니터링할 수 있는 태핑(Tapping) 장비를 설치하고, 네트워크 패킷 중 데이터베이스 질의문을 확인하여 이를 로그로 남김

#### 1) [그림 2-29] 모니터링 툴을 이용한 데이터베이스 로그 생성과 보존



### 학습내용3 : 응용 프로그램의 로그 관리

#### 1. IIS 웹 서버의 로그

- \* IIS(Internet Information Services) 웹 서버의 로그 확인
- : [제어판]-[관리 도구]-[IIS(인터넷 정보 서비스) 관리자]-[IIS] 창에서 '로깅' 항목을 통해 확인할 수 있음

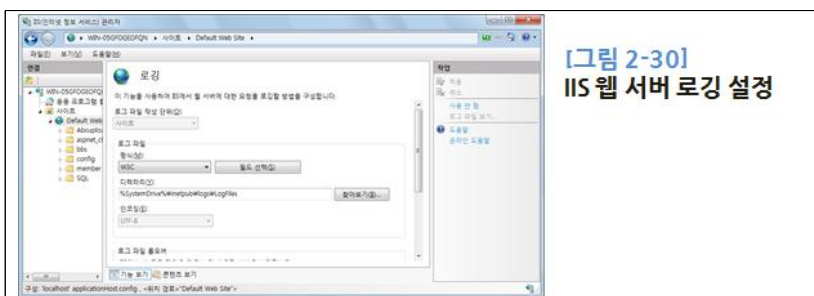


그림 2-30  
IIS 웹 서버 로깅 설정

- \* IIS 웹 서버에서 로그는 기본 W3C 형식으로 남도록 설정되어 있음
- \* W3C 형식 이외에도 다음의 로그 파일 형식을 사용할 수 있음
- NCSA
- IIS
- 사용자 지정 방식



## 2. IIS 웹 서버의 로그인

### 1) W3C 로그 형태

```
2012-06-03 08:53:12 192.168.137.128 GET
/XSS/GetCookie.asp?cookie=ASPSESSIONIDQCAQDDA 80 - 192.168.137.1
Mozilla/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;) 200 0 0 225
```

- 날짜와 시간 : 2012-06-03 08:53:12
- 서버 IP : 192.168.137.128
- HTTP 접근 방법과 접근 URL : GET /XSS/GetCookie.asp?cookie=ASPSESSIO...
- 서버 포트 : 80
- 클라이언트 IP : 192.168.137.1
- 클라이언트의 웹 브라우저 : Mozilla/5.0 + (compatible;+MSIE +9.0;+Windows..
- 실행 결과 코드 : 200(OK)
- 서버에서 클라이언트로 전송한 데이터 크기 : 0
- 클라이언트에서 서버로 전송한 데이터의 크기 : 0
- 처리 소요 시간 : 225 밀리세컨드

## 3. 아파치 웹 서버의 로그

<아파치 웹 서버에 대한 기본 접근 로그는 access\_log에 남으며, 형식은 'combined'로 지정됨>

### 1) [표 2-7] Combined 형식 로그에 사용되는 인수

인자	내용	인자	내용
%a	클라이언트의 IP 주소	%A	서버 IP 주소
%b	헤더 정보를 제외하고서 전송된 데이터의 크기, 전 송된 데이터의 크기가 0일 때 '-'로 표시	%c	응답이 완료되었을 때의 연결 상태 <ul style="list-style-type: none"> <li>• X : 응답이 완료되기 전에 연결이 끊김</li> <li>• + : 응답이 보내진 후에도 연결이 지속됨</li> <li>• - : 응답이 보내진 후 연결이 끊김</li> </ul>
%[Header]e	환경 변수 헤더의 내용	%f	요청된 파일 이름

인자	내용	인자	내용
%h	클라이언트의 도메인 또는 IP 주소	%H	요청 프로토콜의 종류
%i	inetd를 사용하고 있을 때 클라이언트의 로그인명	%m	요청 방식
%p	서버가 요청을 받아들이는 포트 번호	%P	요청을 처리하는 자식 프로세스의 ID
%q	질의에 사용된 문자	%r	HTTP 접근 방법과 접근 URL
%s	HTTP 실행 결과 코드	%{format}t	웹 서버에 작업을 요구한 시간

인자	내용	인자	내용
%T	웹 서버가 요청을 처리하는 데 소요된 시간 (초)	%u	클라이언트의 사용자
%U	요청된 URL 경로	%v	요청을 처리하는 서버의 이름
%i	클라이언트의 웹 브라우저		

## 2) access\_log 형태

```
192.168.137.1 -- [06/JUN/2012:05:48:28 +0900] "GET / HTTP/1.1" 403 4609 "-"
"Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)"
```

- 클라이언트 IP(%h) : 192.168.137.1
- 클라이언트 로그인명(%l) : -
- 클라이언트 사용자명(%u) : -
- 날짜와 시간(%t) : [06/JUN/2012:05:48:28 +0900]
- HTTP 접근 방법과 접근 URL(%r) : GET / HTTP/1.1
- 실행 결과 코드(%s) : 403 Forbidden
- 서버에서 클라이언트로 전송한 데이터 크기(%b) : 4609 바이트
- 클라이언트의 웹 브라우저(%i) : Mozilla/5.0 (compatible; MSIE 9.0; Windows...

## 학습내용4 : 네트워크 장비의 로그 관리

### 1. 네트워크 보안 시스템의 로그

- 침입 차단 시스템, 침입 탐지 시스템, 침입 방지 시스템 등 다양한 보안 시스템의 로그를 확인할 수 있음
- 다양한 보안 시스템의 로그는 통합로그관리시스템(SIEM, Security Information and Event Management)에 의해 수집되고 관리되기도 함

### 2. 네트워크 관리 시스템의 로그

<침입 차단 시스템, 침입 탐지 시스템, 침입 방지 시스템 등 다양한 보안 시스템의 로그를 확인할 수 있음  
다양한 보안 시스템의 로그는 통합로그관리시스템(SIEM, Security Information and Event Management)에 의해 수집되고 관리되기도 함>

### 3. 네트워크 장비 인증 시스템의 로그

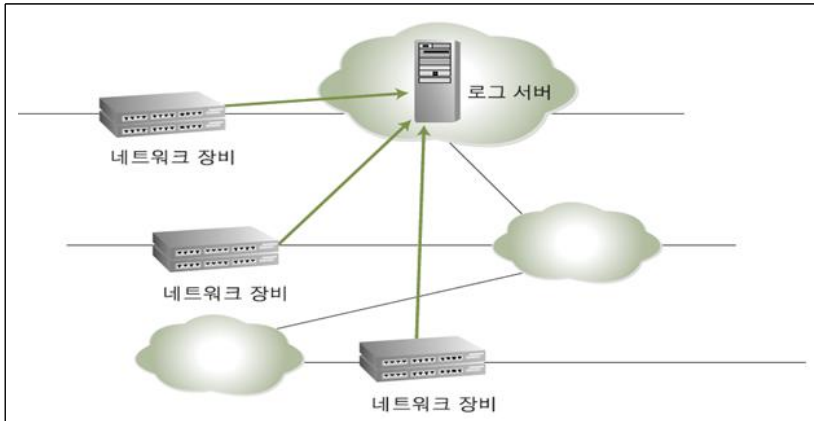
<대규모 네트워크를 운영하는 곳에서는 라우터나 스위치의 인증을 일원화하기 위해 인증 서버로 TACACS+(Terminal Access Controller Access-Control System Plus)를 사용하기도 함>

- 이 인증 서버를 통해서 네트워크 장비에 대한 인증 시도 및 로그인 정보 등을 확인할 수 있음

#### 4. 네트워크 장비의 로그 생성과 보존

- 라우터나 스위치는 자체적으로 로그를 남기는 저장공간이 없음
- 각 네트워크 장비에서 생성되는 로그를 네트워크를 통해 로그 서버에 전송
- 해커가 어떤 네트워크 장비에 침투하더라도 자신의 흔적을 지우기가 쉽지 않음

##### 1) [그림 2-33] 네트워크 장비의 로그 생성과 보존



#### 【학습정리】

1. 로그관리는 Authentication(인증), Authorization(인가), Accounting 으로 구성된다.
2. 윈도우는 이벤트(Event)라고 불리는 중앙 집중화된 형태로 로그를 관리한다.
3. 유닉스의 로그관리는일반적으로 중앙 집중화되어 관리되지 않고, 분산되어 생성된다.
4. 로그관리의 응용에는 운영체제 로그관리, 데이터베이스 로그관리, 응용프로그램 로그관리, 네트워크장비의 로그관리 등이 있다.