# 3.3.日誌管理

### 3.3.1.日誌log|日誌管理|日誌分析

### 3.3.2.windows作業系統日誌及其管理

```

Windows日誌分三種

1. 系統日誌

2. 安全日誌

3. 應用程式日誌

Windows採binary(二進制)對日誌文件存儲

通常也只用Windows事件查看器(event viewer)或第三方日誌分析工具讀取

```

```

1.Windows 2000 Advanced Server

應用程式：C:\WINNT\system32\config\Appevent.Evt

安全：C:\WINDOWS\System32\config\SecEVENT.Evt

系統：C:\WINDOWS\System32\config\SysEvent.Evt

2.Windows Server 2003企業版

應用程式：C:\WINDOWS\system32\config\Appevent.Evt

安全：C:\WINDOWS\System32\config\SecEVENT.Evt

系統：C:\WINDOWS\System32\config\SysEvent.Evt

3.Windows Server 2008 標準版

應用程式：%SystemRoot%\System32\Winevt\Logs\Application.evtx

安全：%SystemRoot%\System32\Winevt\Logs\Security.evtx

系統： %SystemRoot%\System32\Winevt\Logs\System.evtx

4.windows Vista\Windows 7\windows 8\windows 10 日誌情況

應用程式：%SystemRoot%\System32\Winevt\Logs\Application.evtx

安全：%SystemRoot%\System32\Winevt\Logs\Security.evtx

系統： %SystemRoot%\System32\Winevt\Logs\System.evtx

```

### 3.3.3.Linux作業系統日誌及其管理

```

UNIX/LINUX分三個子系統:

(1) 登陸時間日誌子系統 存放在var/log/wtm和var/run/utmp

(2) 行程統計日誌子系統

(3) 錯誤日誌子系統 存放在/var/log/messages/

由Sysloge操作(新版用rsyslogd)

```

```

UNIX/Linux日誌文件格式:

1. 基於syslogd的日誌文件

Syslogd依優先程度分8級 0~7

通常是ASCII碼的文件格式

2. 應用程式產生的日誌

通常是ASCII碼的文件格式

程式會將日誌傳往syslogd並統一處理

```

```

大部分應用層的日誌會儲存在/var/log/messages/

Apache的日誌 會儲存於/var/log/httpd/access\_log

Samba 則儲存在/var/log/samba

```

```

操作紀錄日誌文件分兩類

1.對登陸人員進行記錄的lastlog

2.系統郵件伺服器運行時紀錄的maillog

```

### 3.3.4.Apache網站伺服器日誌及其管理

```

Apache默認日誌位置在 Apache配置文件/etc/apache2/apache2.conf中定義為

Customlog/var/log/apache2/access\_log.combined

```