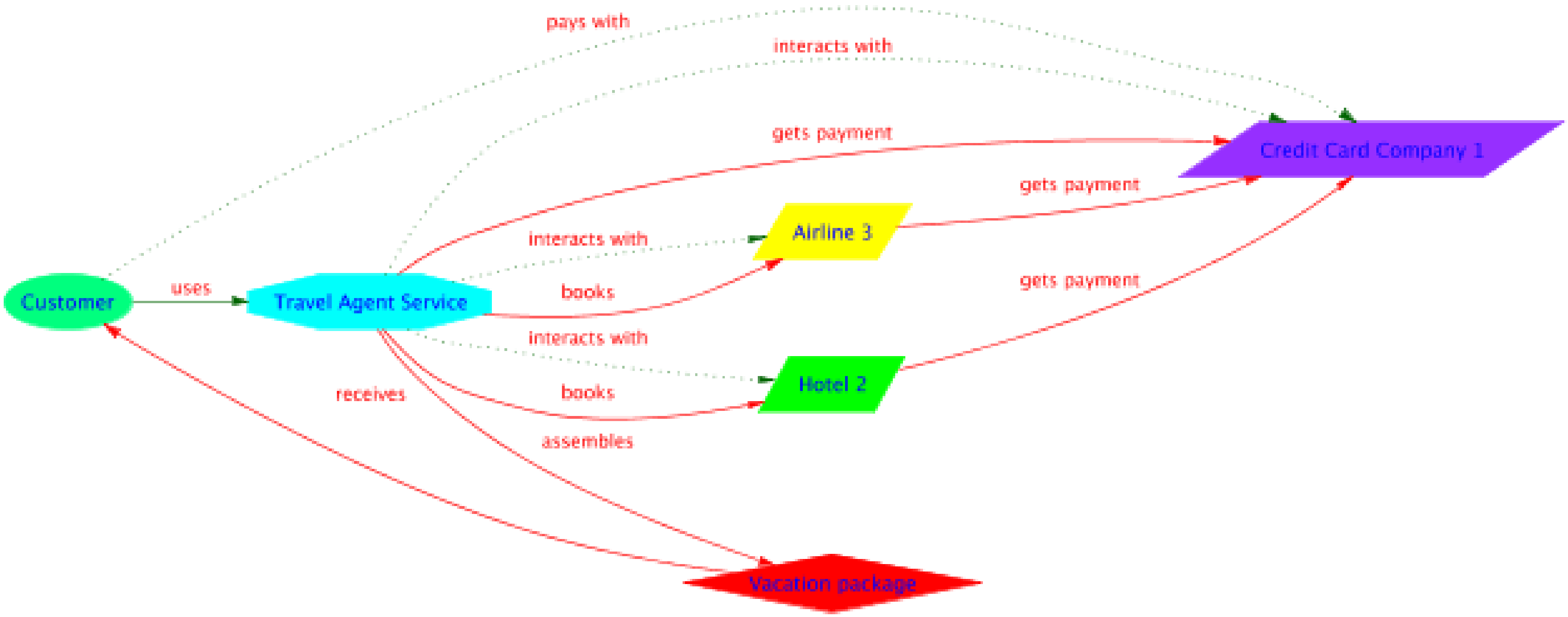
ST2610

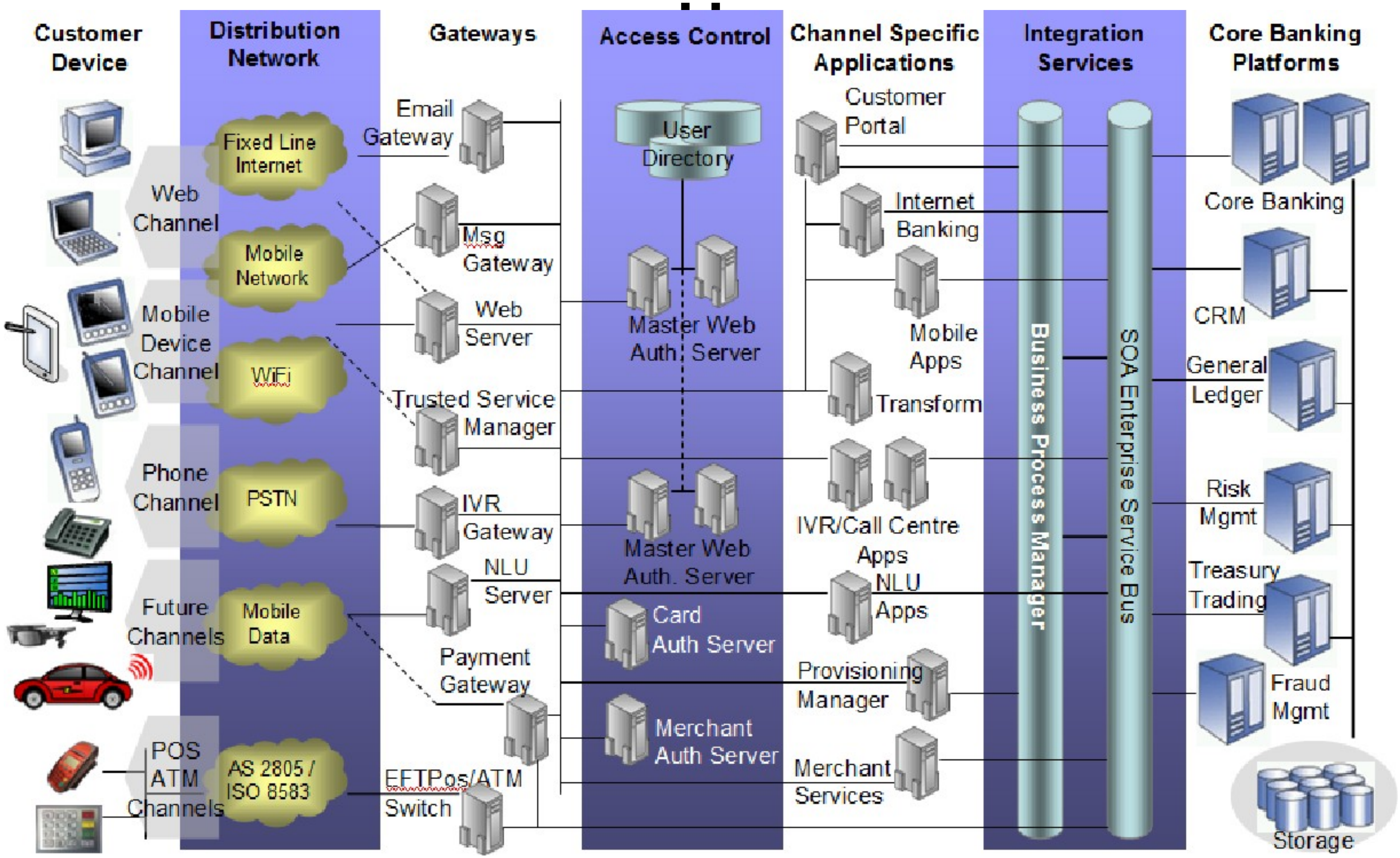
Security **P**olicies and **I**ncident **M**anagement

Elephant in the Room

CYBER SECURITY
©2013 Telos Corporation

Value Chain of a IT Business Service




Customer Device
Distribution Network
Gateways
Access Control
Channel Specific Applications
Integration Services
Core Banking Platforms
Web Channel
Mobile Device Channel
Phone Channel
Future Channels
POS ATM Channels
Fixed Line Internet
Mobile Network
WiFi
PSTN
Mobile Data
AS 2805 / ISO 8583
Email Gateway
Msg Gateway
Web Server
Trusted Service Manager
IVR Gateway
NLU Server
Payment Gateway
EFTPos/ATM Switch
User Directory
Master Web Auth. Server
Master Web Auth. Server
Card Auth Server
Merchant Auth Server
Customer Portal
Internet Banking
Mobile Apps
Transform
IVR/Call Centre Apps
NLU Apps
Provisioning Manager
Merchant Services
Business Process Manager
SOA Enterprise Service Bus
Core Banking
CRM
General Ledger
Risk Mgmt
Treasury Trading
Fraud Mgmt
Storage

Elephant in the Room Problem

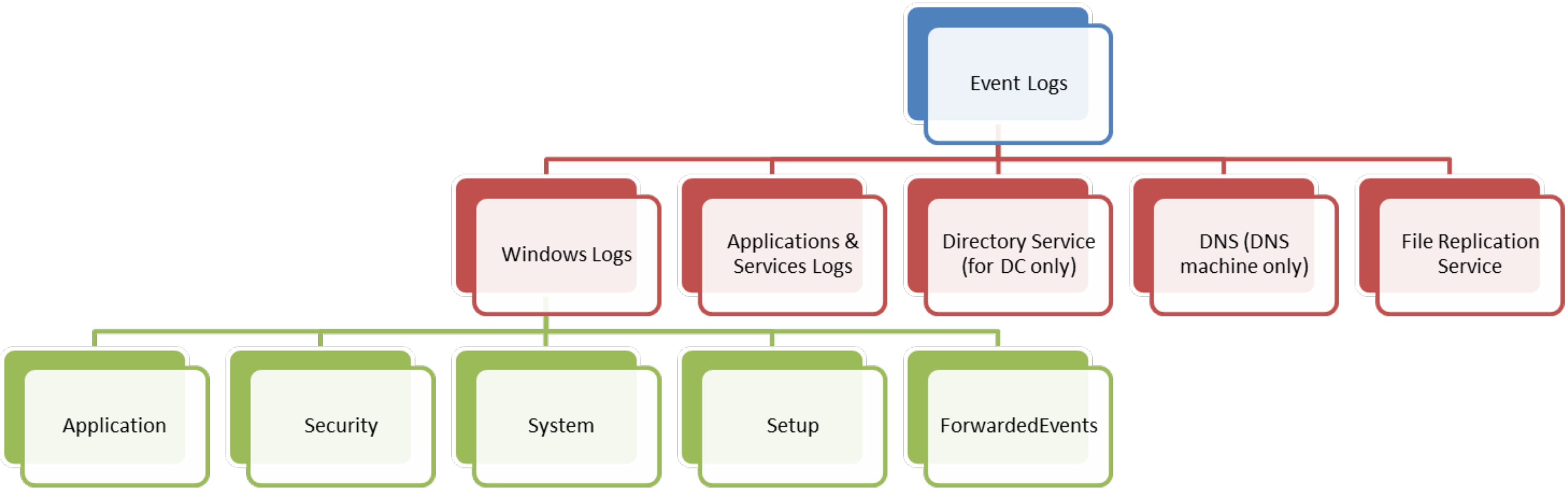
- Multiple systems, multiple platforms
- Some on-site, some off-site, some in the cloud
- When something goes wrong, where do you go to find out what went wrong, how it went wrong, when it went wrong etc..

Log Messages

Server Operating System

- Windows-based
  - E.g. Windows Server 2012, windows server 2008, etc.
- Unix-based
  - E.g. IBM AIX, HP UX, Solaris, OS X
- Linux-based
  - E.g. Redhat Enterprise Linux, SUSE, Ubuntu
- Others
  - z/OS (IBM)

Windows Server Logging



Application Log

- Contain events logged by applications or programs
  - a database program might record a file error in the application log
- Program developers decide which events to log

Security Log

- Contains events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files or other objects.
- Administrators can specify what events are recorded in the security log.
  - e.g. if enabled logon auditing, attempts to log on to the system are record (specified in audit policy)
- One of the primary tools used by Administrators to detect and investigate attempted and successful unauthorized activity and to troubleshoot problems

Security Log

- The log and the audit policies that govern it are also favourite targets of hackers and rogue system administrators seeking to cover their tracks before and after committing unauthorized activity
- If the audit policy is set to record logins, a successful login results in the user's user name and computer name being logged as well as the user name they are logging into. Depending on the version of Windows and the method of login, the IP address may or may not be recorded. Windows 2000 Web Server, for instance, does not log IP addresses for successful logins, but Windows Server 2003 includes this capability

Security Log

- The categories of events that can be logged are:
- Account logon events
- Account management
- Directory service access
- Logon events
- Object access
- Policy change
- Privilege use
- Process tracking
- System events

System Log

- Contains events logged by Windows system components.
  - E.g. the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined by Windows.

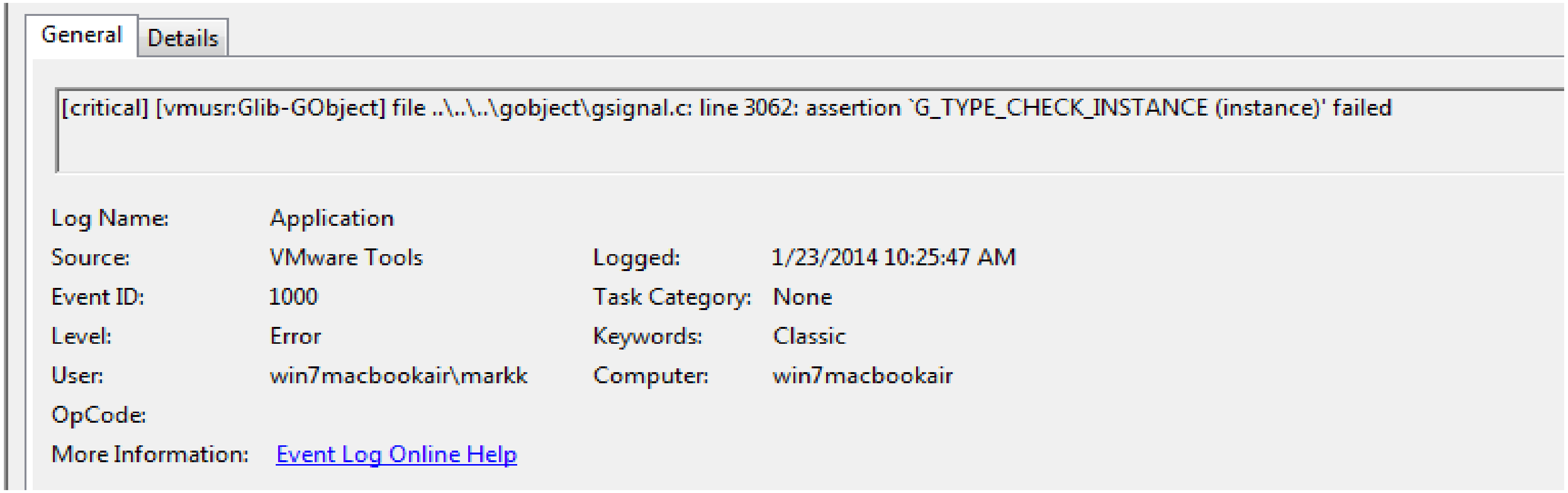
Applications and Services Logs

- Store events from a single application or component rather than events that might have system-wide impact.

Event Properties

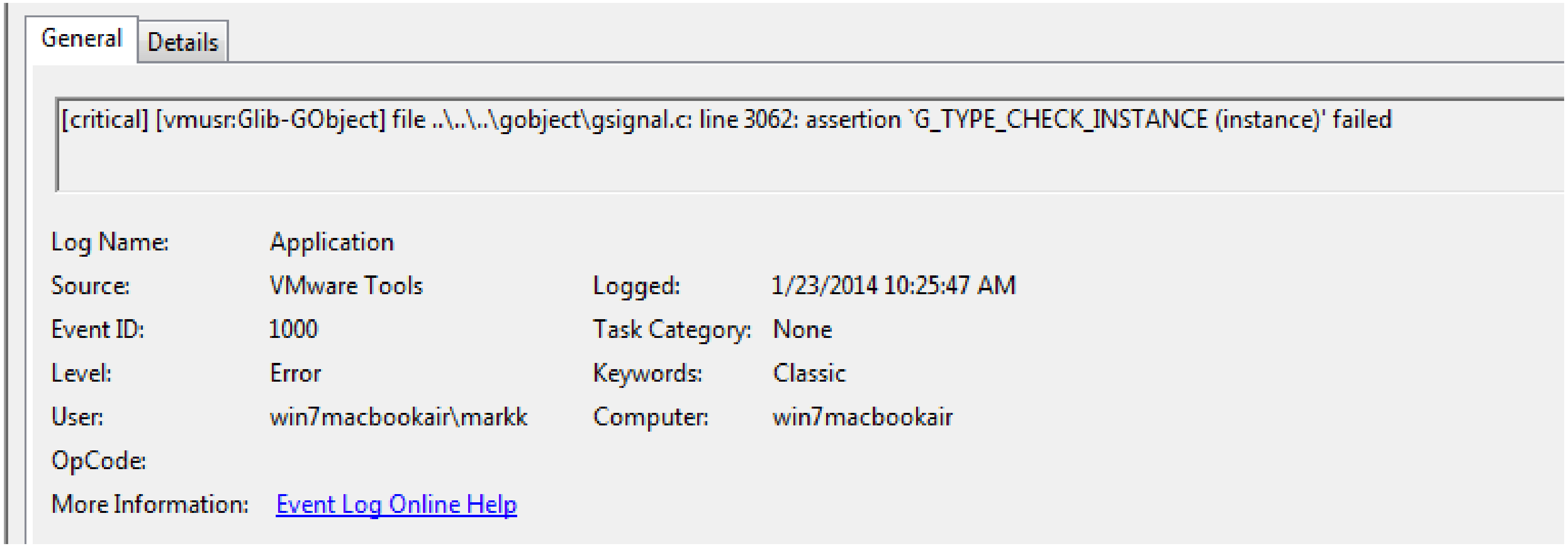
Property Name	Description
Source	The software that logged the event
Event ID	A number identifying the particular event type
Level	**Information, Warning, Error, Critical** **Success Audit**, **Failure Audit** (indicates that the exercise of a user right has succeeded/failed, in security log)
User	name of the user on whose behalf the event occurred. Client ID if the event was actually caused by a server process or the primary ID if impersonation is not taking place.
Operational Code	Contains a numeric value that identifies the activity or a point within an activity that the application was performing when it raised the event.
Log	The name of the log where the event was recorded
Task Category	a subcomponent or activity of the event publisher.
Keyword	A set of categories or tags that can be used to filter or search for events.
Computer	The name of the computer on which the event occurred. The computer name is typically the name of the local computer, but it might be the name of a computer that forwarded the event or it might be the name of the local computer before its name was changed.
Date & Time	The date and time that the event was logged.

Examples



```
[critical] [vmusr:Glib-GObject] file ..\..\..\gobject\gsignal.c: line 3062: assertion `G_TYPE_CHECK_INSTANCE (instance)' failed
```

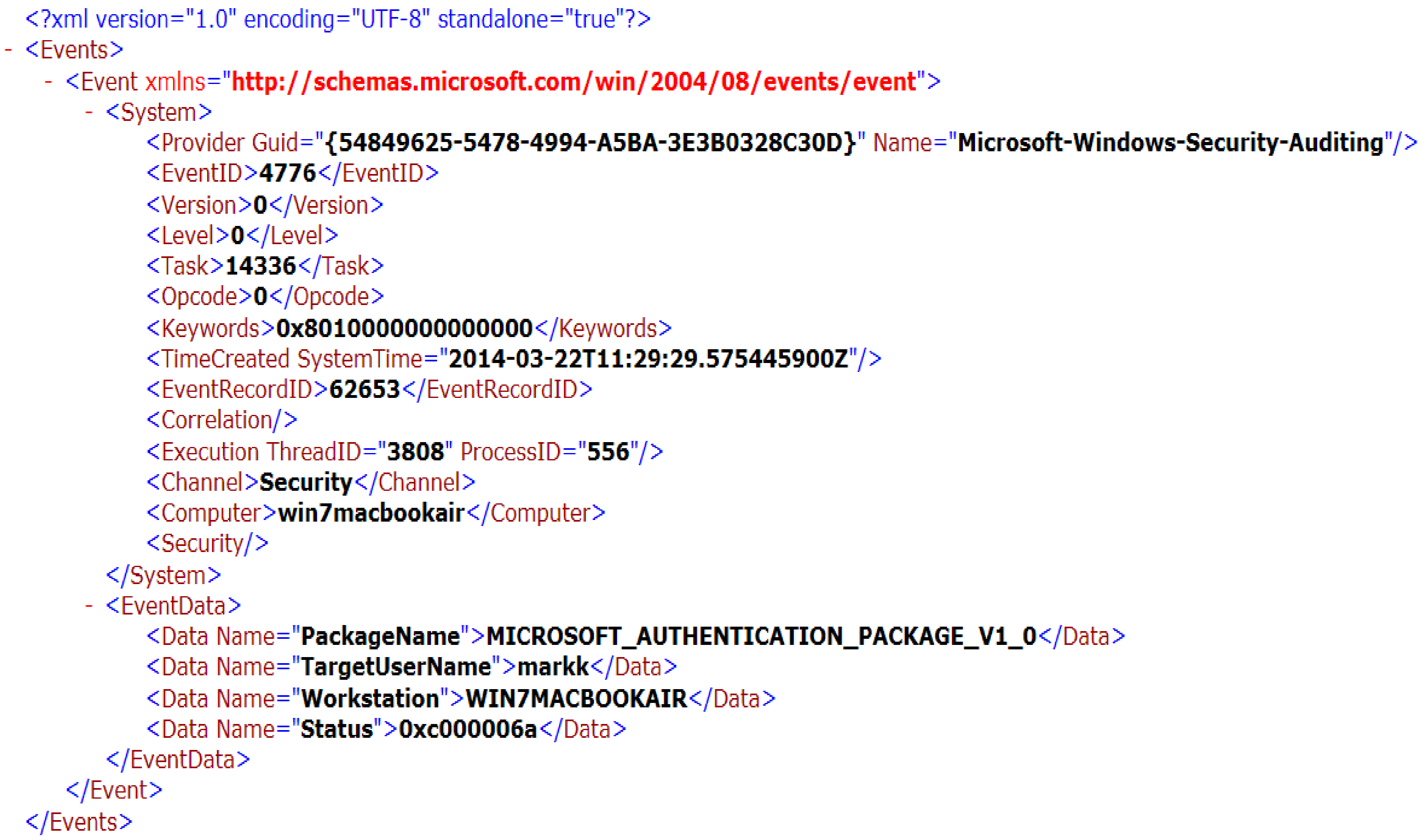
Log Name: Application
Source: VMware Tools   Logged: 1/23/2014 10:25:47 AM
Event ID: 1000   Task Category: None
Level: Error   Keywords: Classic
User: win7macbookair\markk   Computer: win7macbookair
OpCode:
More Information: Event Log Online Help


General
Details

[critical] [vmusr:Glib-GObject] file ..\..\..\gobject\gsignal.c: line 3062: assertion `G_TYPE_CHECK_INSTANCE (instance)' failed

Log Name: Application
Source: VMware Tools   Logged: 1/23/2014 10:25:47 AM
Event ID: 1000   Task Category: None
Level: Error   Keywords: Classic
User: win7macbookair\markk   Computer: win7macbookair
OpCode:
More Information: Event Log Online Help

Event (in XML)



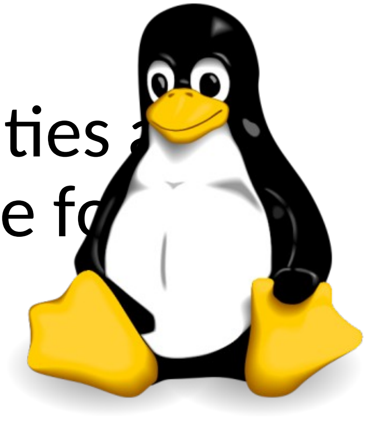
```
  <?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <Events>
  - <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
    - <System>
        <Provider Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" Name="Microsoft-Windows-Security-Auditing"/>
        <EventID>4776</EventID>
        <Version>0</Version>
        <Level>0</Level>
        <Task>14336</Task>
        <Opcode>0</Opcode>
        <Keywords>0x8010000000000000</Keywords>
        <TimeCreated SystemTime="2014-03-22T11:29:29.575445900Z"/>
        <EventRecordID>62653</EventRecordID>
        <Correlation/>
        <Execution ThreadID="3808" ProcessID="556"/>
        <Channel>Security</Channel>
        <Computer>win7macbookair</Computer>
        <Security/>
      </System>
    - <EventData>
        <Data Name="PackageName">MICROSOFT_AUTHENTICATION_PACKAGE_V1_0</Data>
        <Data Name="TargetUserName">markk</Data>
        <Data Name="Workstation">WIN7MACBOOKAIR</Data>
        <Data Name="Status">0xc000006a</Data>
      </EventData>
    </Event>
  </Events>
```

Location of Logs

- Default locations:
  - %SystemRoot%\System32\Winevt\Logs\Application.evtx
  - %SystemRoot%\System32\Winevt\Logs\Security.evtx
  - %SystemRoot%\System32\Winevt\Logs\System.evtx
- Default locations can be changed using regedit or EventViewer

Linux Operating System

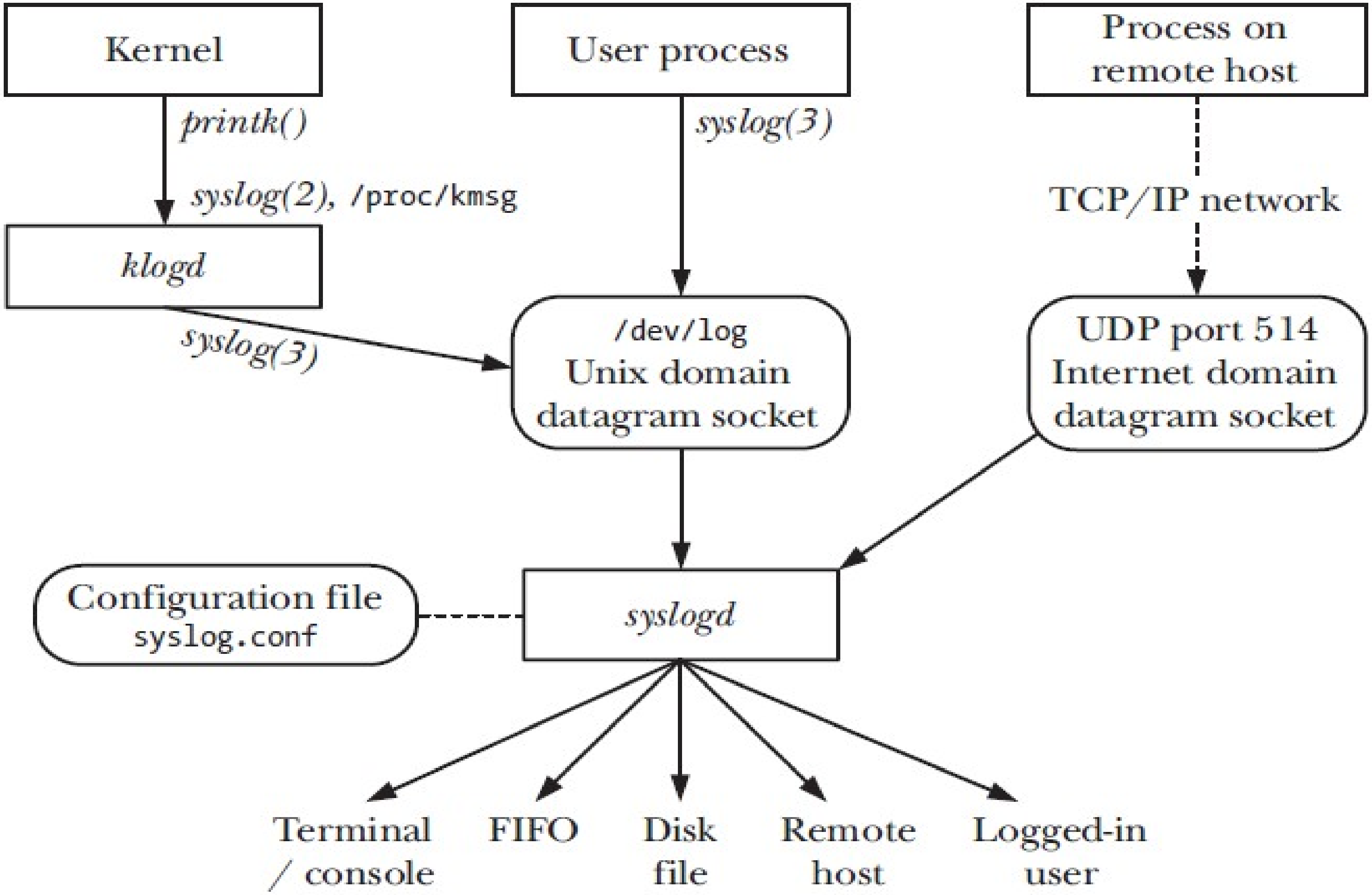
- Unix-like POSIX compliant operating system
- Open source (under GNU General Public License)
- Usually package as different Linux distributions
  - E.g. Debian, Ubuntu, Linux Mint, Fedora, Arch Linux, and the commercial Red Hat Enterprise Linux and SUSE Linux Enterprise Server.
  - include the Linux kernel, supporting utilities a libraries and various application software fo intended use



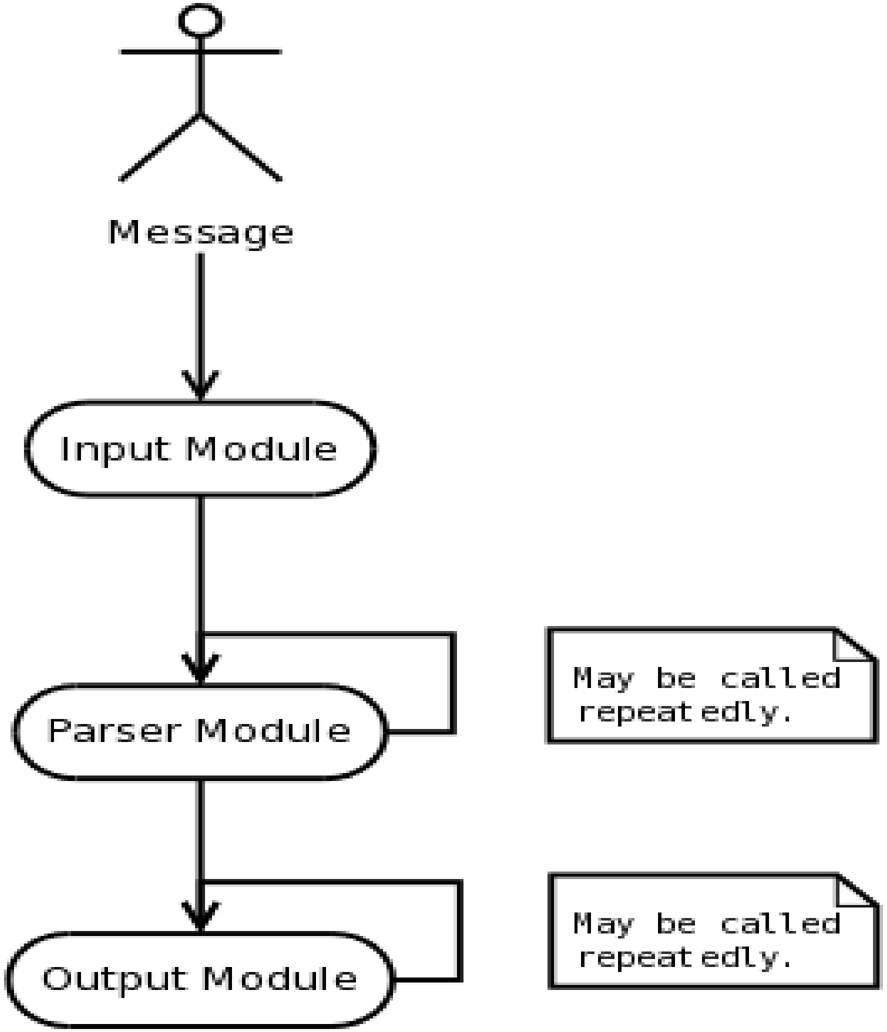
Linux Log Management

- Most Linux applications uses **syslog** or **rsyslog** utility for logging
- Log files are usually stored in /var/log directory
- Configuration file for syslog is /etc/syslog.conf and for rsyslog is /etc/rsyslog.conf
- Rsyslog implements the basic syslog protocol, extends it with content-based filtering, rich filtering capabilities, flexible configuration options and adds important features such as using TCP for transport

Syslog


Kernel
printk()
syslog(2), /proc/kmsg
klogd
syslog(3)
User process
syslog(3)
/dev/log
Unix domain
datagram socket
Process on
remote host
TCP/IP network
UDP port 514
Internet domain
datagram socket
Configuration file
syslog.conf
syslogd
Terminal
/ console
FIFO
Disk
file
Remote
host
Logged-in
user

Rsyslog Architecture



Rsyslog rules

- Consist of two columns
  - 1st column: list the facilities and severities of messages
  - 2nd column: the files to which they should be logged to
- Severity level
  - Emergencies, alerts, critical, errors, warnings, notifications, informational, debugging

Rsyslog rules

- Rules
  - Facility/priority-based filters
  - Facility refers to subsystem that produces a specific syslog message, e.g. mail, auth, authpriv, cron, daemon, kern, lpr, news, syslog, user, uucp, local0 to local7, etc
  - Priority (debug, info, notice, warn, err, crit, alert, emerg)
- Examples:
  - `kern.*` (selects all kernel syslog messages with any priority)
  - `mail.crit` (selects all mail syslog messages with priority crit and higher)
  - `cron.!info, !debug` (selects all cron syslog messages except those with info or debug priority)

Rsyslog filter

- Property-based filters

  :<property>, [!]<compare_operation>, “<String>”

  e.g.

  :`msg,contains,“error”` -> selects syslog messages which contain the string error in message txt

- Expression-based filters

  If (expression> then <action>

  e.g. `$msg startswith ‘DEVNAME’`

Rsyslog actions

- Actions
  - Saving syslog messages to log files
    - E.g `cron.*    /var/log/cron.log`
  - Sending syslog messages over network
    - `*.*   @192.168.0.1` #forwards messages to 192.168.0.1 via UDP protocol
    - `*.*   @@example.com:18` #forwards messages to example.com using port 18 and TCP protocol

Linux Auditing

- Linux kernel traps auditable events and writes them to buffers where they are processed by auditd daemon.
  - e.g. Pluggable Authentication Modul (PAM) repots login related events to audit log
- Admin can control what event and acitivity are audited by /etc/audit/audit.rules and auditctl command.

Linux Log Files

- Some common Linux log files and their default locations
  - /var/log/messages : General message and system related stuff
  - /var/log/auth.log : Authenication logs
  - /var/log/kern.log : Kernel logs
  - /var/log/cron.log : Crond logs (cron job)
  - /var/log/maillog : Mail server logs
  - /var/log/qmail/ : Qmail log directory (more files inside this directory)
  - /var/log/httpd/ : Apache access and error logs directory
  - /var/log/lighttpd/ : Lighttpd access and error logs directory
  - /var/log/boot.log : System boot log
  - /var/log/mysqld.log : MySQL database server log file
  - /var/log/secure or /var/log/auth.log : Authentication log
  - /var/log/utmp or /var/log/wtmp : Login records file
  - /var/log/yum.log : Yum command log file.

Internet Information Services (IIS)

- Extensible web server created by Microsoft for use with Windows NT family
- IIS supports HTTP, HTTPS, FTP, FTPS, SMTP and NNTP
- IIS versions
  - IIS 6.0 (Windows Server 2003)
  - IIS 7.0 (Windows Server 2008)
  - IIS 7.5 (Windows Server 2008 R2)
  - IIS 8.0 (Windows Server 2012)
  - IIS 8.5 (Windows Server 2012 R2)

IIS Logs

- Logging can be set to log per site or per entire server
- Log formats
  - IIS (Fixed ASCII text-based format, not customizable)
  - W3C (World Wide Web Consortium log format, most widely used, default log format, customizable)
  - NCSA (National Center for Supercomputing Applications, default log format for Apache web server, ASCII text-based, not customizable)
- Configurable using
  - IIS Manager (UI)
  - Appcmd

W3C Log Format

- Default location:
  - `%systemdrive%\inetpub\logs\logfiles\W3SVC1.`
  - The number after W3SVC designates the site ID of the website.
- Log rotation:
  - log file can be created hourly, daily, weekly or monthly or based on maximum size
  - Use local server time or Coordinated Universal Time (UTC) for file naming and rollover

IIS Log Naming

Log Interval	W3C Extended	NCSA	IIS
Hourly	exyymmddhh.log	ncyymmddhh.log	Inyymmddhh.log
Daily	exyymmdd.log	ncyymmdd.log	Inyymmdd.log
Weekly	exyymmww.log	ncyymmww.log	Inyymmww.log
Monthly	exyymm.log	ncyymm.log	Inyymm.log
Size	extendnn.log	ncsann.log	Inetsvnn.log

W3C log fields

- Date (date): the date on which the request occurred
- Time (time): the time, in Coordinated Universal Time (UTC), at which the request occurred.
- Client IP Address (c-ip): the IP address of the client that made the request.
- User Name (cs-username): the name of the authenticated user who accessed your server. Anonymous users are indicated by a hyphen.
- Service Name (s-sitename): the site instance number that fulfilled the request.
- Server Name (s-computername): the name of the server on which the log file entry was generated.
- Server IP Address (s-ip): the IP address of the server on which the log file entry was generated.
- Server Port (s-port): the server port number that is configured for the service.
- Method (cs-method): the requested action, for example, a GET method.
- URI Stem (cs-uri-stem): the Universal Resource Identifier, or target, of the action.

W3C log fields

- URI Query (cs-uri-query): the query, if any, that the client was trying to perform. A Universal Resource Identifier (URI) query is necessary only for dynamic pages
- Protocol Status (sc-status): the HTTP or FTP status code.
- Protocol Sub-status (sc-substatus): the HTTP or FTP substatus code.
- Win32 Status (sc-win32-status): the Windows status code.
- Bytes Sent (sc-bytes): the number of bytes that the server sent.
- Bytes Received (cs-bytes): the number of bytes that the server received.
- Time Taken (time-taken): the length of time that the action took in milliseconds.
- Protocol Version (cs-version): the protocol version, HTTP or FTP, that the client used.
- Host (cs-host): the host name, if any.
- User Agent (cs(UserAgent)): the browser type that the client used.
- Cookie (cs(Cookie)): the content of the cookie sent or received, if any.
- Referer (cs(Referer)): the site that the user last visited. This site provided a link to the current site.

W3C Log Sample

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0 #Date: 2009-06-11 05:12:03 #Fields: date time
s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port
cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-
win32-status 2009-06-11 05:12:02 W3SVC1893743816
192.168.1.109 GET / - 4677 - 192.168.1.109 Mozilla/4.0
(compatible;+MSIE+4.01;+Windows+NT;+MS+Search+5.0+Robot)
401 2 2148074254 2009-06-11 05:12:02 W3SVC1893743816
192.168.1.109 GET / - 4677 - 192.168.1.109 Mozilla/4.0+
(compatible;+MSIE+4.01;+Windows+NT;+MS+Search+5.0+Robot)
401 2 2148074254 - See more at:
http://www.surfray.com/blog/2009/08/11/iis-log-file-
formats-overview/#sthash.GaXCsZkQ.dpuf
```

Apache HTTP Server

- One of the most popular web server
- Developed under the auspices of Apache Software Foundation
- Supports a variety of features, many implemented as compiled modules which extend the core functionality, ranging from server-side programming language support to authentication schemes.
  - Common language interfaces support Perl, Python, Tcl, and PHP.
  - Popular authentication modules include mod_access, mod_auth, mod_digest, and mod_auth_digest, the successor to mod_digest.
  - Other features include Secure Sockets Layer and Transport Layer Security support (mod_ssl), a proxy module (mod_proxy), a URL rewriter (mod_rewrite), custom log files (mod_log_config), and filtering support (mod_include and mod_ext_filter).

Apache HTTP Server logs

- Types of logs
  - Error log
    - diagnostic information and record any errors that it encounters in processing requests.
    - Default name: error_log (unix) or error.log (windows)
  - Access Log
    - records all HTTP requests processed by the server.

Access Logs

- The location and content of the access log are controlled by the CustomLog directive
- **Common Log Format**
  - A typical configuration for the access log might look as follows:

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
CustomLog logs/access_log common
```

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif
HTTP/1.0" 200 2326
```

Common Log Format

- 127.0.0.1 (%h) - This is the IP address of the client (remote host) which made the request
- - (%l) - The "hyphen" in the output indicates that the requested piece of information is not available. In this case, this is the userid of the person requesting the document as determined by HTTP authentication
- [10/Oct/2000:13:55:36 -0700] (%t) - The time that the request was received. The format is: [day/month/year:hour:minute:second zone]
- “GET /apache_pb.gif HTTP/1.0" - The request line from the client is given in double quotes
- 200 (%>s) - This is the status code that the server sends back to the client.
- 2326 (%b) - The last part indicates the size of the object returned to the client, not including the response headers

For full-list of log format, see:

http://httpd.apache.org/docs/2.4/mod/mod_log_config.html#formats

Combined Log Format

- Combined Log Format
  - – Another commonly used format string

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
combined
CustomLog log/access_log combined
```

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif
HTTP/1.0" 200 2326 "http://www.example.com/start.html" "Mozilla/4.08 [en]
(Win98; I ;Nav)"
```

Combined Log Format

- "http://www.example.com/start.html" (\"%{Referer}i\") - The "Referer" HTTP request header. This gives the site that the client reports having been referred from. (This should be the page that links to or includes /apache_pb.gif).

- "Mozilla/4.08 [en] (Win98; I ;Nav)" (\"%{User-agent}i\") - The User-Agent HTTP request header. This is the identifying information that the client browser reports about itself.

Forensic Log

- **mod_log_forensic** provides for forensic logging of client requests.
- Logging is done before and after processing a request, so the forensic log contains two log lines for each request.
- The forensic logger is very strict with no customizations. It can be an invaluable debugging and security tool.

```
+yQtJf8CoAB4AAFNXBIEAAAAA|GET /manual/de/images/down.gif HTTP/1.1|
Host:localhost%3a8080|User-Agent:Mozilla/5.0 (X11; U; Linux i686; en-US; rv
%3a1.6) Gecko/20040216 Firefox/0.8|Accept:image/png, etc...
```

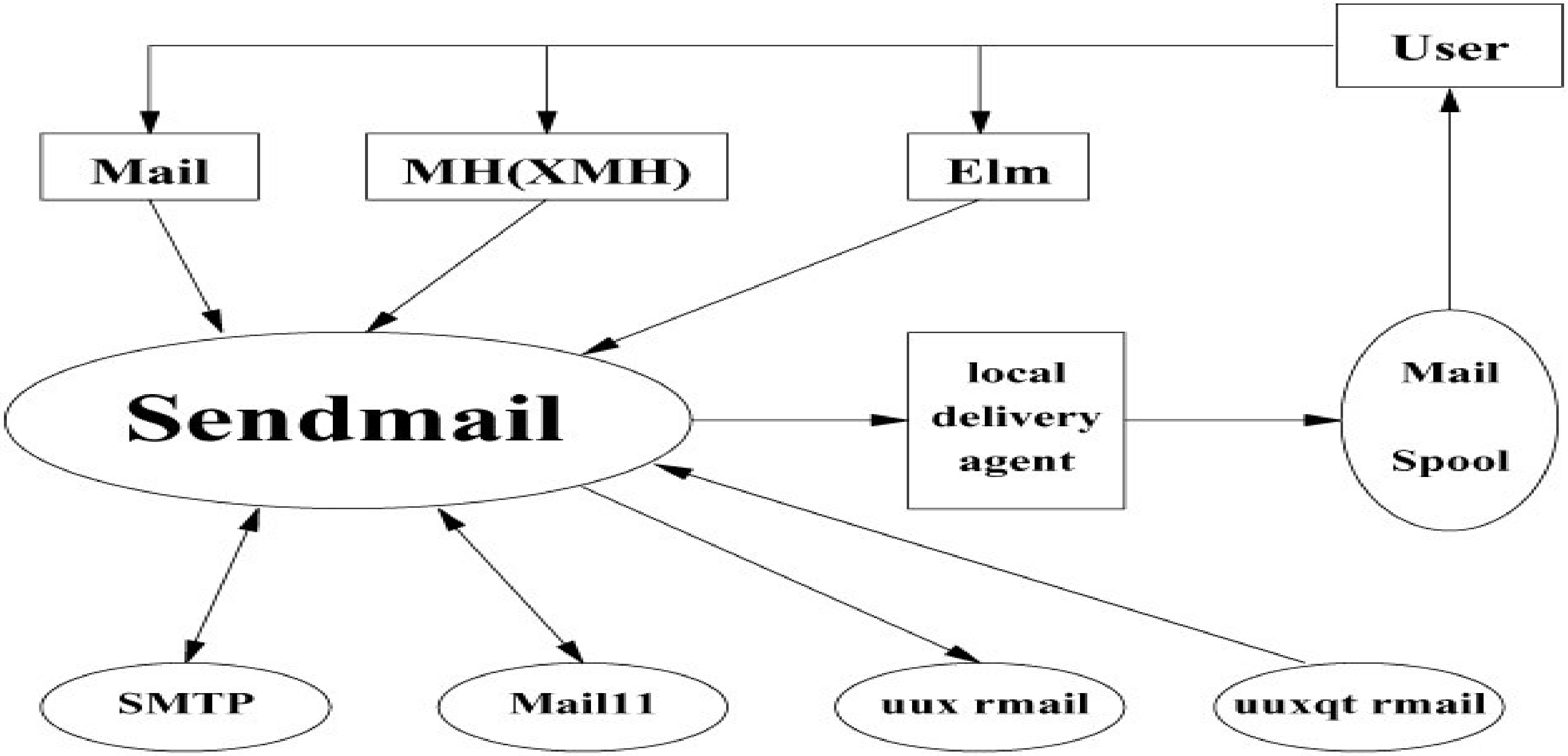
The first line logs the forensic ID, the request line and all received headers, separated by pipe characters (|). A sample line looks like the following (all on one line):

The plus character at the beginning indicates that this is the first log line of this request. The second line just contains a minus character and the ID again:

```
-yQtJf8CoAB4AAFNXBIEAAAAA
```

Sendmail

- Email handling program on Unix/Linux systems



Terminology

- **User Agents**
  - UA is an application run directly by a user. User agents are used to compose and send out-going messages as well as to display, file and print messages which have arrived in a user's mail-box
- **Transfer Agents**
  - Mail transfer agents (MTAs) are used to transfer messages between machines. User agents give the message to the transfer agent, who may pass it onto another transfer agent, or possibly many other transfer agents.
  - Transfer agents are responsible for properly routing messages to their destination. Sendmail is an example of MTA
- **Delivery Agents**
  - Delivery agents are used to place a message into a user's mail-box. When the message arrives at its destination, the final transfer agent will give the message to the appropriate delivery agent, who will add the message to the user's mail-box.

Sendmail Log

- Sendmail uses the syslog(3) facility to log its activities. The syslog facility used is "mail“
- The log message contents depends on the sendmail version
- The general format of a sendmail message log line is:

```
<date> <host> sendmail[pid]: <qid>: <message>
```

  - Most message is in name=value pair
  - A line is logged per message received and per delivery attempt

Receipt of Message Log

Field	Description
class	The class (i.e., numeric precedence) of the message
pri	The initial message priority (used for queue sorting).
nrcpts	The initial message priority (used for queue sorting).
msgid	The message id of the message (from the header).
bodytype	The message body type (7BIT or 8BITMIME), as determined from the envelope.
proto	The protocol used to receive this message (e.g., ESMTP or UUCP)
daemon	The daemon name from the DaemonPortOptionssetting
relay	The machine from which it was received.

Delivery Log

Field	Description
To	A comma-separated list of the recipients to this mailer
ctladdr	The “controlling user”, that is, the name of the user whose credentials we use for delivery.
Delay	The total delay between the time this message was received and the current delivery attempt
xdelay	The amount of time needed in this delivery attempt (normally indicative of the speed of the connection).
Mailer	The name of the mailer used to deliver to this recipient.
relay	The name of the host that actually accepted (or rejected) this recipient.
dsn	The enhanced error code (RFC 2034) if available.
stat	Delivery status

Examples

```
Jul 15 17:11:21 thor.foo.com sendmail[22398]: e6FFBLP22398:
from=<jan(a)foo.com>, size=589, class=0, nrcpts=1,
msgid=<200007151510.e6FFAC316448(a)odin.foo.com>, proto=ESMTP,
daemon=MTA, relay=jan(a)odin.foo.com [192.168.1.1]

Jul 15 17:11:21 thor.foo.com sendmail[22400]: e6FFBLP22398:
to=<gerrit(a)bar.com>, delay=00:00:00, xdelay=00:00:00, mailer=esmtp, pri=30589,
relay=frigga.bar.com. [192.168.1.3], dsn=2.0.0, stat=Sent (e6FFAFv24566 Message
accepted for delivery)
```

Active Directory

- Active Directory Domain Services (AD DS) is Microsoft’s implementation of a directory service that provides centralized authentication and authorization services.
- Centrally store and manage security principals, such as users, groups, and computers, and it offers centralized and secure access to network resources.
- Active Directory makes use of Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

AD Logs

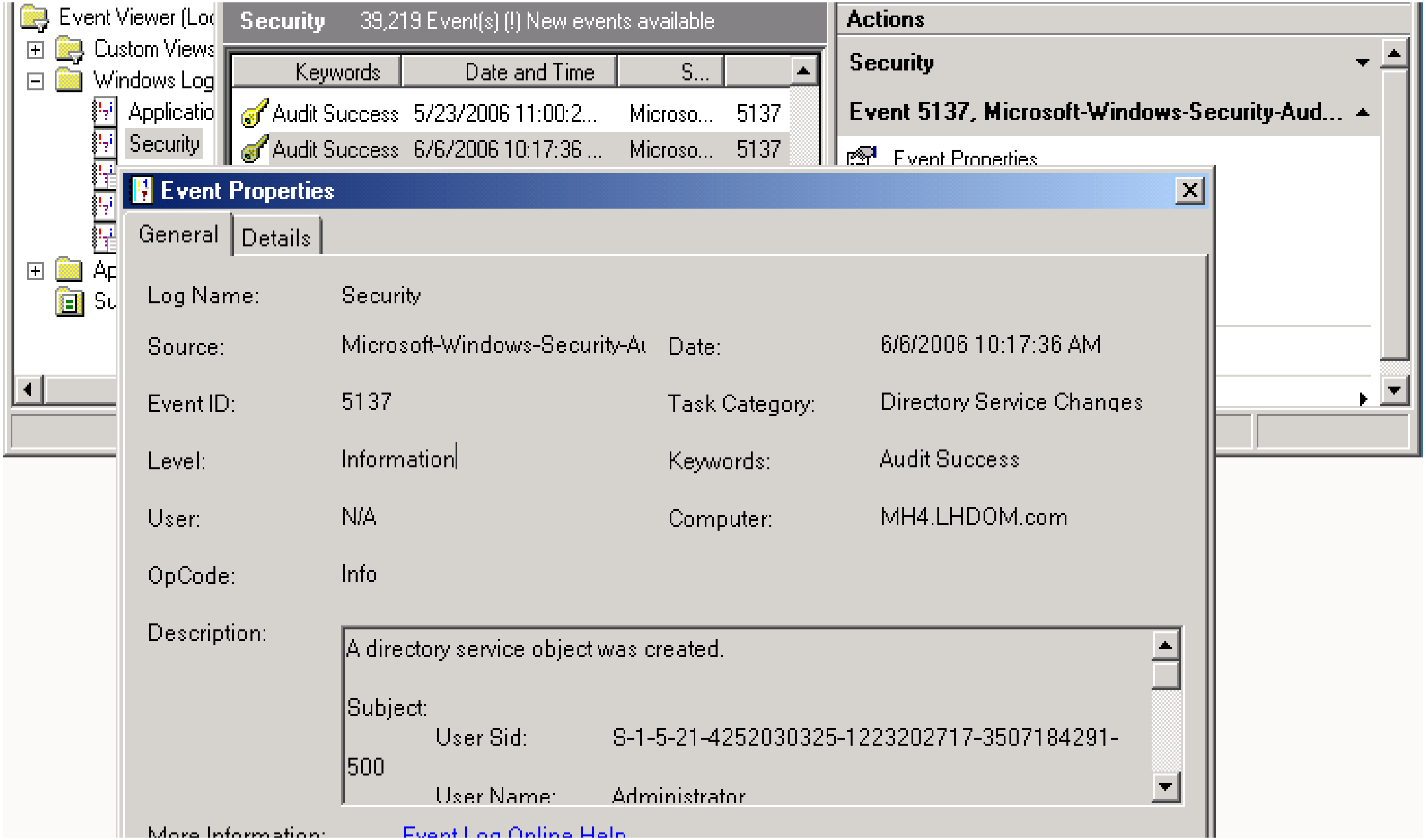
- Two related logs
  - Directory service log
    - contains events logged by the Windows Active Directory service. For example, connection problems between the server and the global catalog are recorded in the directory service log.
  - Security Log
    - security audit logs, such as logon events and directory access/changes etc.

AD Auditing Log

- Must enable auditing of directory access and modifications. Audit events are logged to the security event log
- Categories of audit policies:

- Directory Service Access
- Directory Service Changes
- Directory Service Replication
- Detailed Directory Service Replication

Create a User object



Security 39,219 Event(s) (!) New events available

Keywords	Date and Time	S...	
Audit Success	5/23/2006 11:00:2...	Microso...	5137
Audit Success	6/6/2006 10:17:36 ...	Microso...	5137

Event Properties

Log Name: Security

Source: Microsoft-Windows-Security-Au

Date: 6/6/2006 10:17:36 AM

Event ID: 5137

Task Category: Directory Service Changes

Level: Information

Keywords: Audit Success

User: N/A

Computer: MH4.LHDOM.com

OpCode: Info

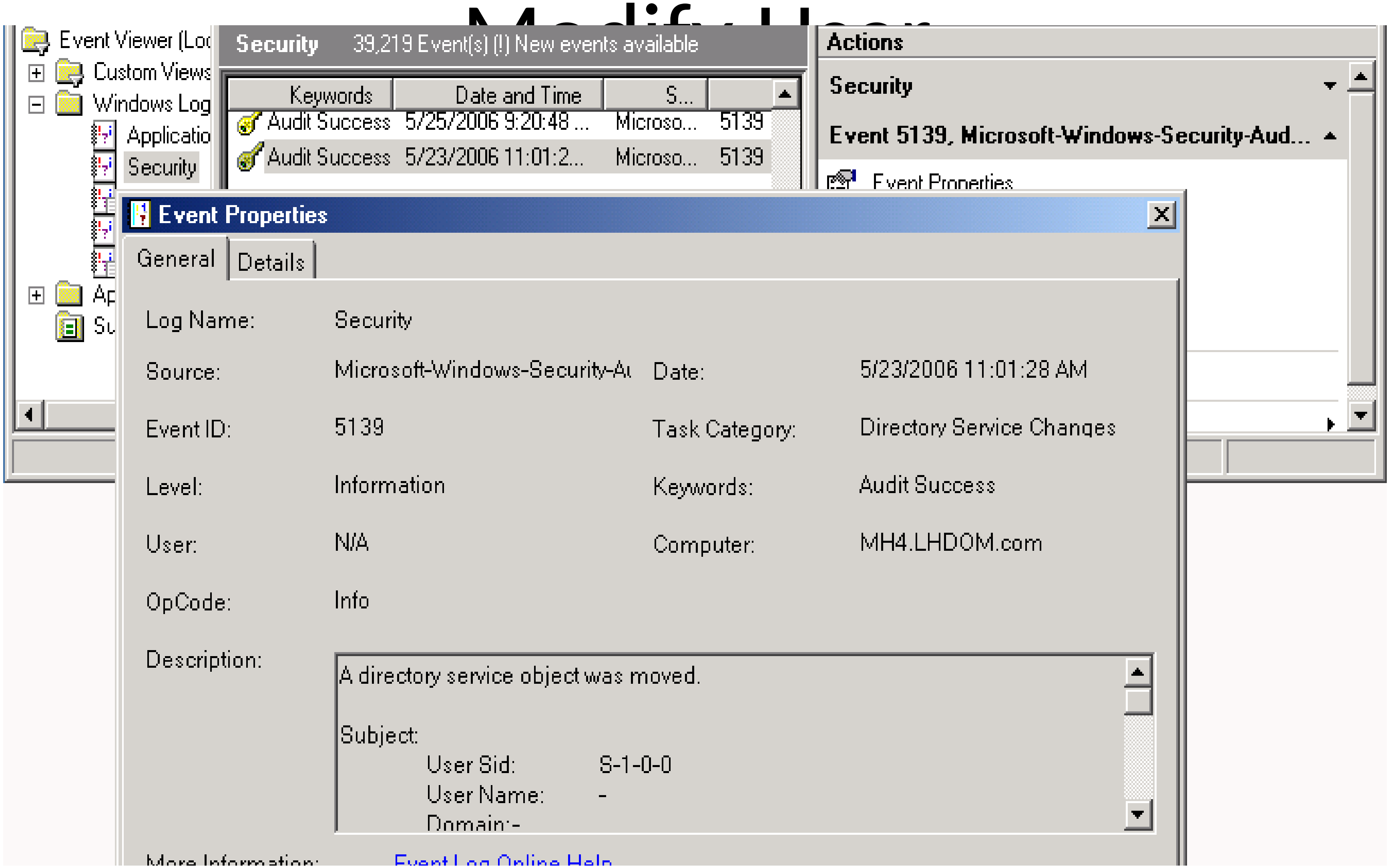
Description:

```
A directory service object was created.

Subject:
        User Sid:        S-1-5-21-4252030325-1223202717-3507184291-
500
        User Name:       Administrator
```

More Information: Event Log Online Help

Modify User



Security 39,219 Event(s) (!) New events available

Keywords	Date and Time	S...	
Audit Success	5/25/2006 9:20:48 ...	Microso...	5139
Audit Success	5/23/2006 11:01:2...	Microso...	5139

Event Properties

Log Name: Security

Source: Microsoft-Windows-Security-Au Date: 5/23/2006 11:01:28 AM

Event ID: 5139 Task Category: Directory Service Changes

Level: Information Keywords: Audit Success

User: N/A Computer: MH4.LHDOM.com

OpCode: Info

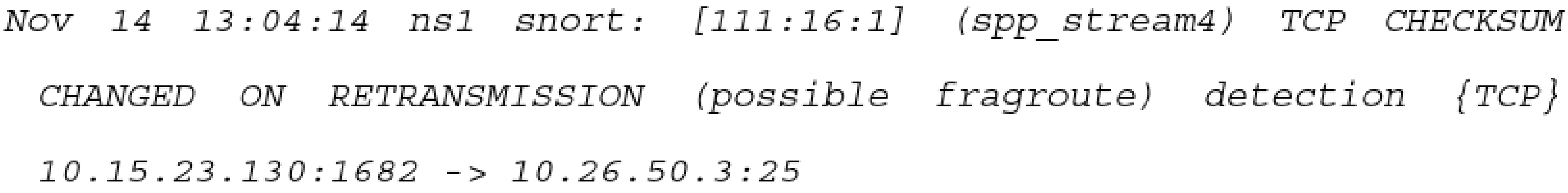
Description:

```
A directory service object was moved.

Subject:
          User Sid:        S-1-0-0
          User Name:       -
          Domain:-
```

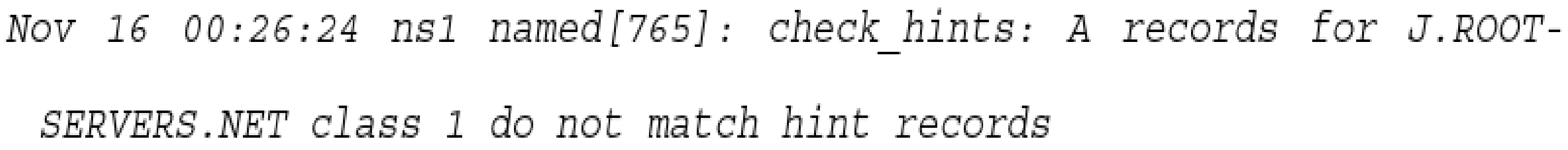
More Information: Event Log Online Help

NIDS Alert Logs (SNORT)



```
Nov 14 13:04:14 ns1 snort: [111:16:1] (spp_stream4) TCP CHECKSUM
  CHANGED ON RETRANSMISSION (possible fragroute) detection {TCP}
  10.15.23.130:1682 -> 10.26.50.3:25
```

DNS Logs



```
Nov 16 00:26:24 ns1 named[765]: check_hints: A records for J.ROOT-
  SERVERS.NET class 1 do not match hint records
```

- One of the root DNS servers has its IP address changed, but this DNS server that produced the above syslog message still has the old information in its configuration file.

Log formats

- Text logs
  - W3C Extended log file format (ELF), Apache access log, Cisco SDEE/CIDEE, ArcSight common event format, Syslog, IDMEF (XML-based format)

- Binary logs
  - Windows event log – evt file in c:\WINDOWS\SYSTEM32\CONFIG\ directory
  - Compressed logs – security by obscurity
  - Relational database

- Open format
  - Documented as ISO, ANSI, or an Internet standard, or in an RFC reference

- Proprietary format

What Logs Should Have

Log message formatting

Useful components of a log entry

- Who? *Username*
  - For user or administrator activities
  - Include name of the identify provider if available
- What? *Object*
  - The affected system component
  - E.g. user account, file
- What? *Status*
  - The action succeeded, failed, or deferred

Log message formatting

- Where? *System*, *application* or *component*
  - Relevant application context
  - E.g. initiator and target systems
- Where? *Source*
  - For network connectivity or distributed application operation
  - IP address or hostname
  - Related components include *destination*, *source port*, and *destination port*

Log message formatting

- When? *Time stamp* and *time zone*
  - Time zone is essential for distributed applications
  - High volume system can also use a transaction ID
- Why? *Reason*
  - Doesn’t require security and audit personnel to dig for a hidden reason
- How? *Action*
  - Provide nature of the event

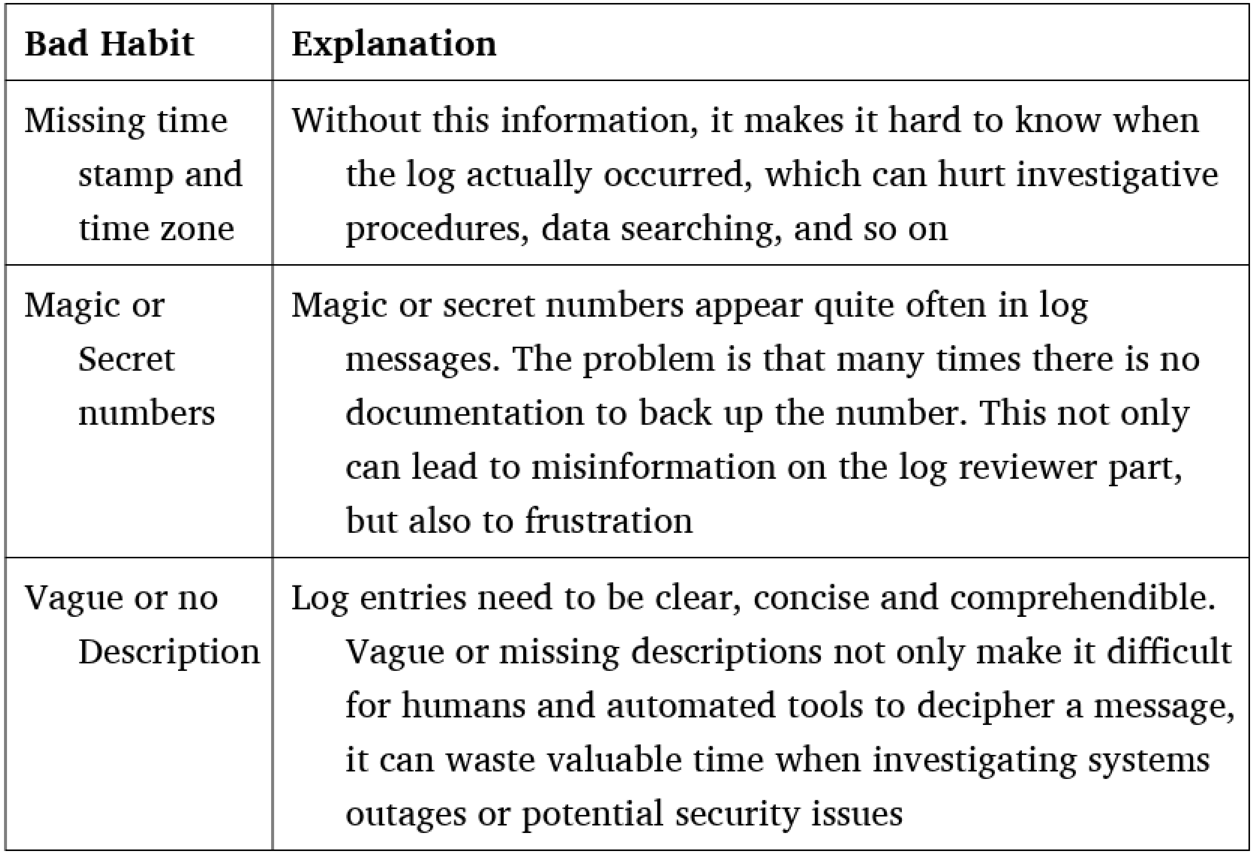
Log message formatting

- How important? *Priority*
  - Different companies can have different policies on information availability vs. confidentiality
- Group related messages: *session id*
  - Group related messages across multiple threads and processes

Log message formatting

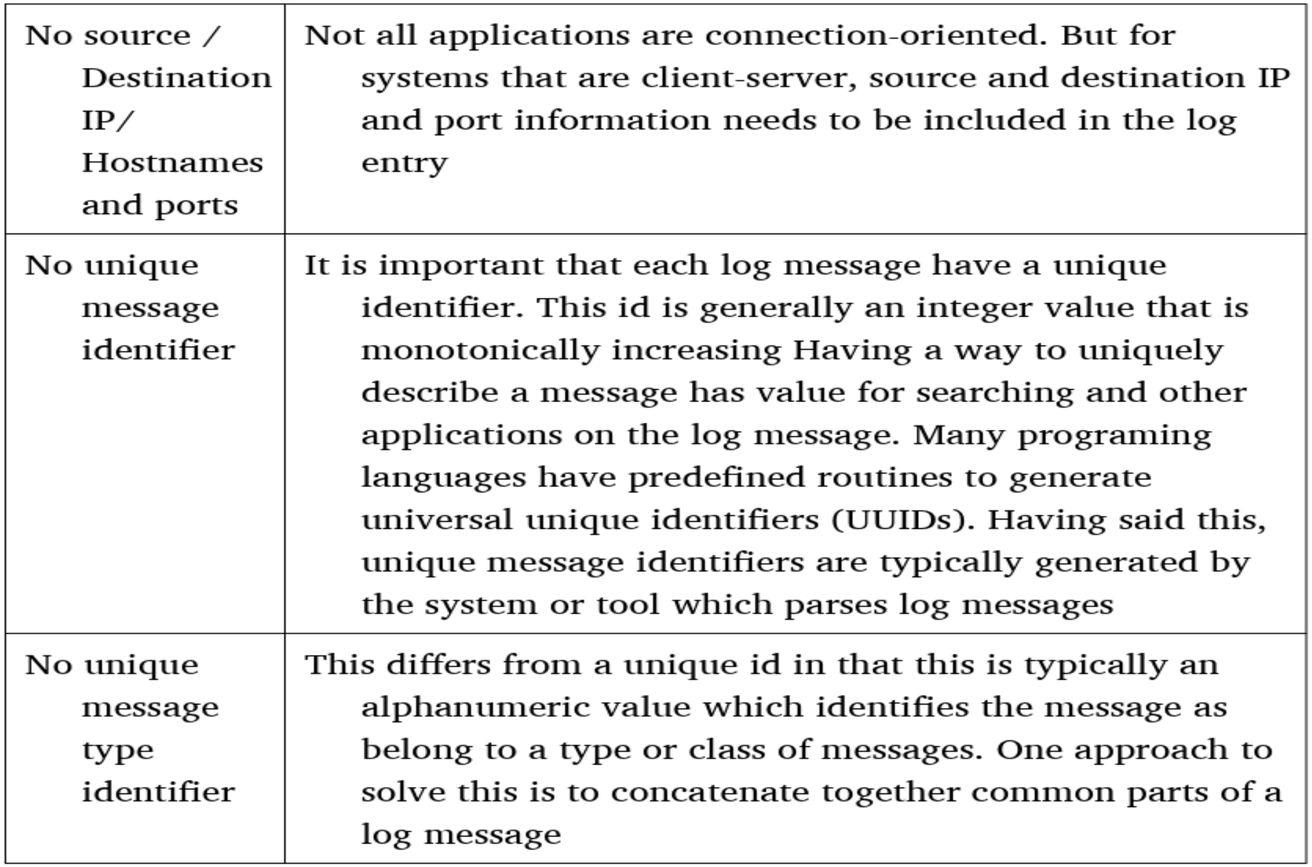
- *process id (pid)* and *thread id (tid):*
  - Correlate a running application with its log records, when multiple applications write to a shared log file
- *Activity measurement*
  - E.g. detect attempts to transfer a larger-than-expected batch of data

Bad habits in logging



Bad Habit	Explanation
Missing time stamp and time zone	Without this information, it makes it hard to know when the log actually occurred, which can hurt investigative procedures, data searching, and so on
Magic or Secret numbers	Magic or secret numbers appear quite often in log messages. The problem is that many times there is no documentation to back up the number. This not only can lead to misinformation on the log reviewer part, but also to frustration
Vague or no Description	Log entries need to be clear, concise and comprehendible. Vague or missing descriptions not only make it difficult for humans and automated tools to decipher a message, it can waste valuable time when investigating systems outages or potential security issues

Bad habits in logging

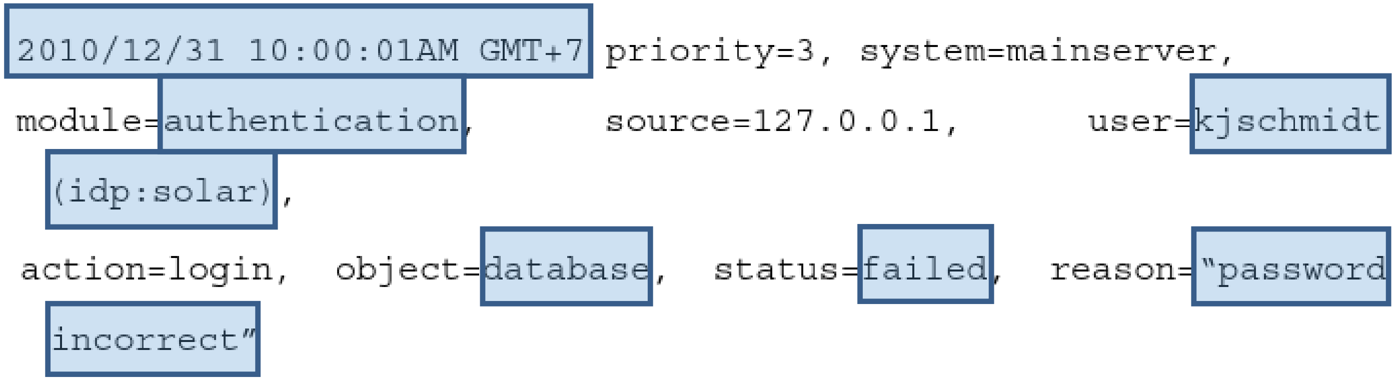


No source / Destination IP/ Hostnames and ports	Not all applications are connection-oriented. But for systems that are client-server, source and destination IP and port information needs to be included in the log entry
No unique message identifier	It is important that each log message have a unique identifier. This id is generally an integer value that is monotonically increasing Having a way to uniquely describe a message has value for searching and other applications on the log message. Many programing languages have predefined routines to generate universal unique identifiers (UUIDs). Having said this, unique message identifiers are typically generated by the system or tool which parses log messages
No unique message type identifier	This differs from a unique id in that this is typically an alphanumeric value which identifies the message as belong to a type or class of messages. One approach to solve this is to concatenate together common parts of a log message

Criteria for good logging

- -------------- Dream to know ----------------------
  - What will happen next
  - What else happened that I should care about
  - What should I do about it
- ---------- Icing on the cake ------------------------
  - Where do I get more info
  - How certain should I be that the above is really what happened
  - What is affected
- ------ 5W's & 1H - essentials of logging -------

Useful log message example



```
2010/12/31 10:00:01AM GMT+7 priority=3, system=mainserver,
module=authentication,     source=127.0.0.1,     user=kjschmidt
  (idp:solar),
action=login,  object=database,  status=failed,  reason="password
  incorrect"
```

- Name=value pairs, separated by comma, giving no ambiguity in parsing

- Who?
- What happened?
- Where?
- When?
- Why?
- How?
  - User entered a bad password

Summary

- Logs come in different formats, but they contain the common important fields
- There is gap between what logs actually contain and what we would like them to contain

Log Management

Log collection planning

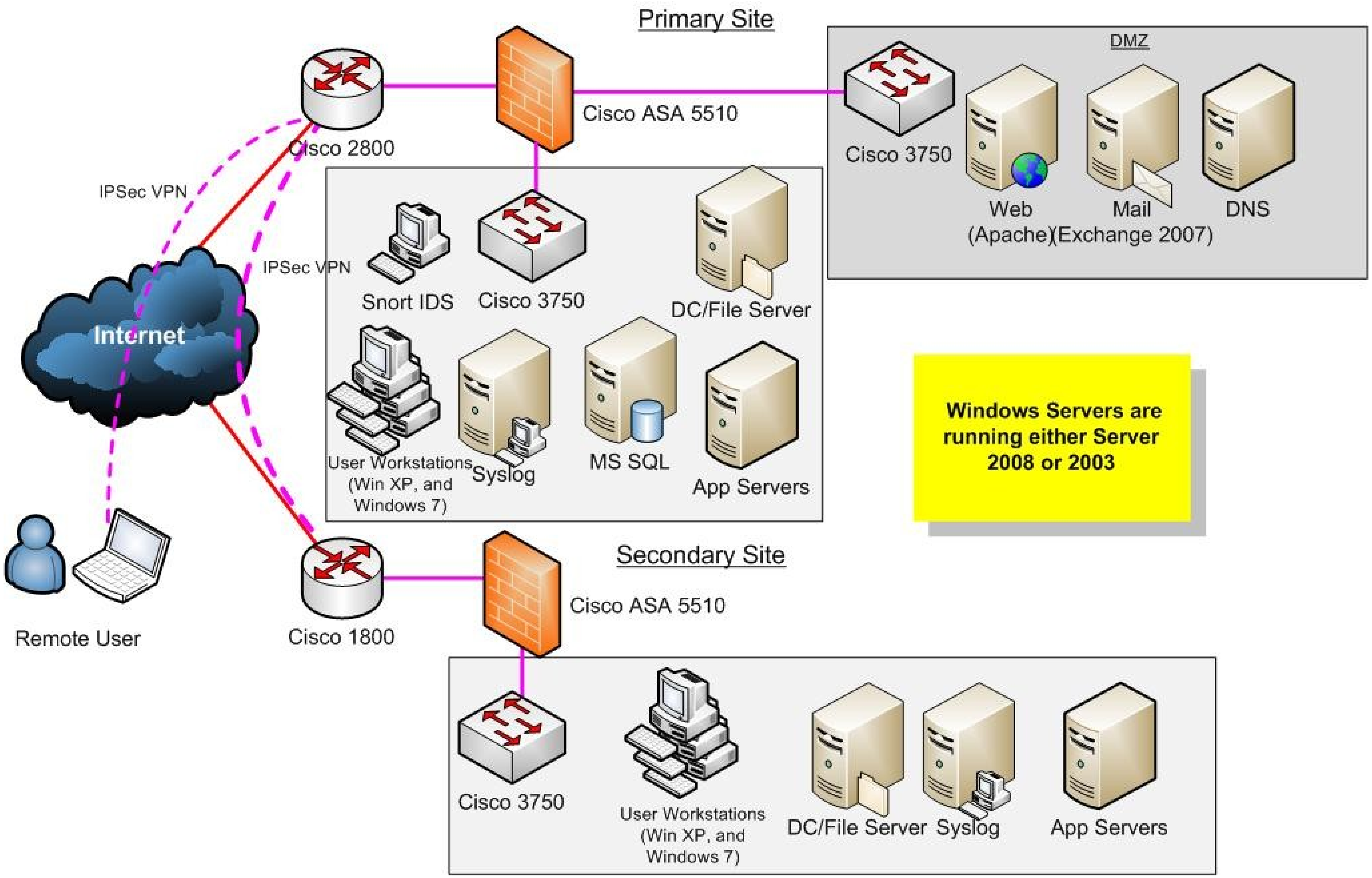
- Identify your exact needs
- Architecture
- Policy definition
- Scalability
- Software selection

Log analysis goals

- Goals of analysis varies depending on your business needs
  - Security and Compliance
- Past bad things
- Future bad things
- Never before seen things

Policy definition

- Logging policy
  - Adequate logging
  - Log aggregation and retention
  - Log protection
  - Log review



Windows Servers are running either Server 2008 or 2003

Security host logs

- Security related host logs
  - Host logs produced by OS components
  - Various network services logs
  - Logs of applications running on the system

Security host logs

- Host logs from applications with a security mission running on a host
  - Related to attacks, intrusions, compromises, infections
  - False alarms

- Host intrusion detection and prevention
  - Detect and block a wide variety of network, operating system and application attacks
  - HIPS block attacks based on signatures, dynamic rules or other mechanisms
  - Events recorded are related to
    - Reconnaissance or probe detected
    - Changes to executable files

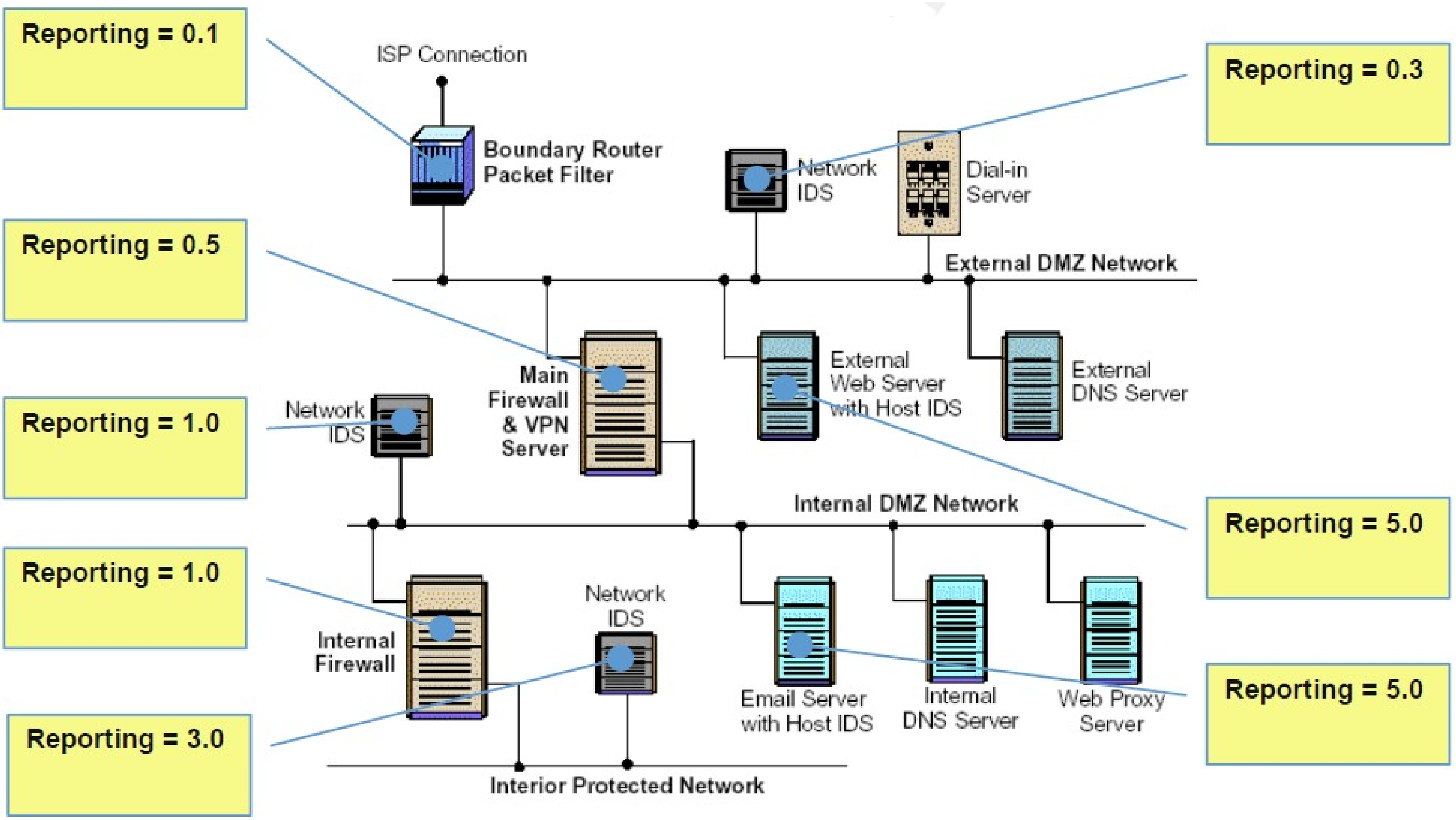
Security related network logs

- Network logs generated by network infrastructure
  - By routers and switches

- Network infrastructure logs
  - Logins and logouts
  - Connection established to the service
  - Bytes transferred in and out
  - Reboots
  - Configuration changes

Selecting log sources

- Establish a repeatable process for evaluating and selecting systems and devices for logging
  - Criticality
    - Assign a criticality level to a device
    - e.g. firewall is more critical than workstation
    - e.g. DNS server will have lower criticality than your credit processing server
  - Validation
    - Get stakeholders to verify together that the source is indeed a critical asset



Reporting = 0.1

Reporting = 0.3

Reporting = 0.5

Reporting = 1.0

Reporting = 5.0

Reporting = 1.0

Reporting = 5.0

Reporting = 3.0

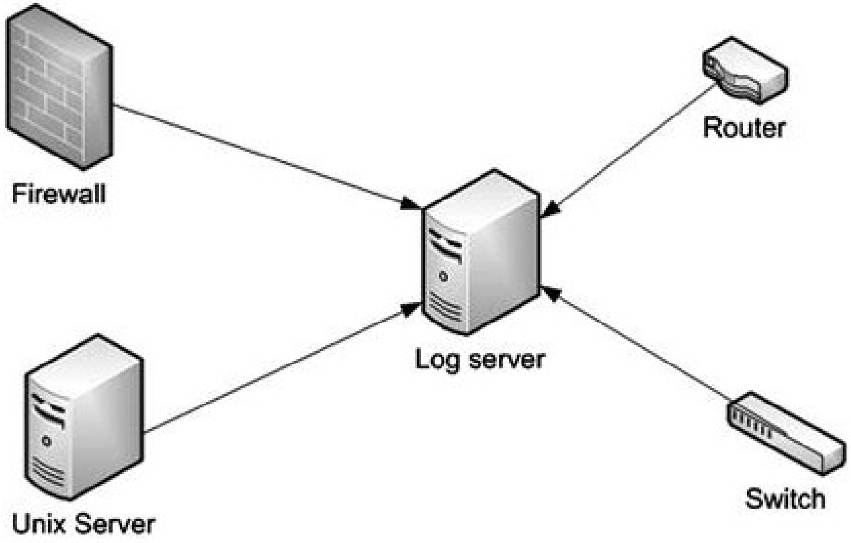
Logging policy on log source selection

- Collect log records from external firewalls and IDS/IPS systems
- Collect log records from every firewall, IPS, server, and desktop in your network
- Review the policy very 3 to 6 months

Architecture

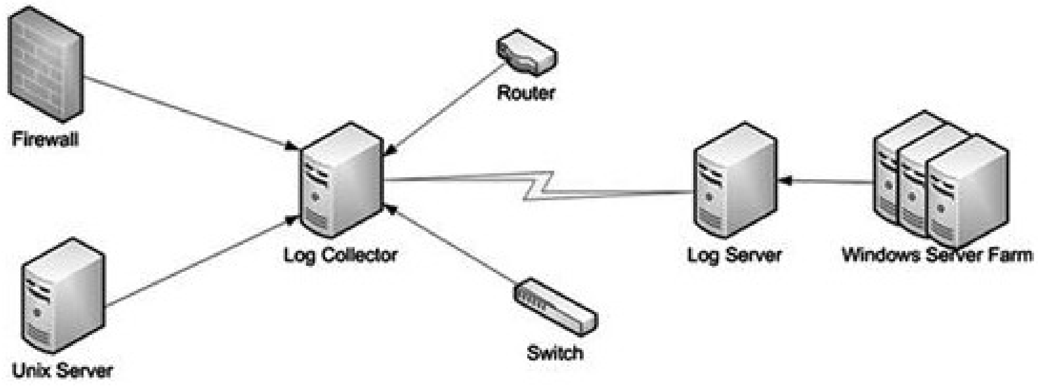
- Basic
- Log server and log collector
- Log server and log collector with long-term storage
- Distributed

Basic log server deployment

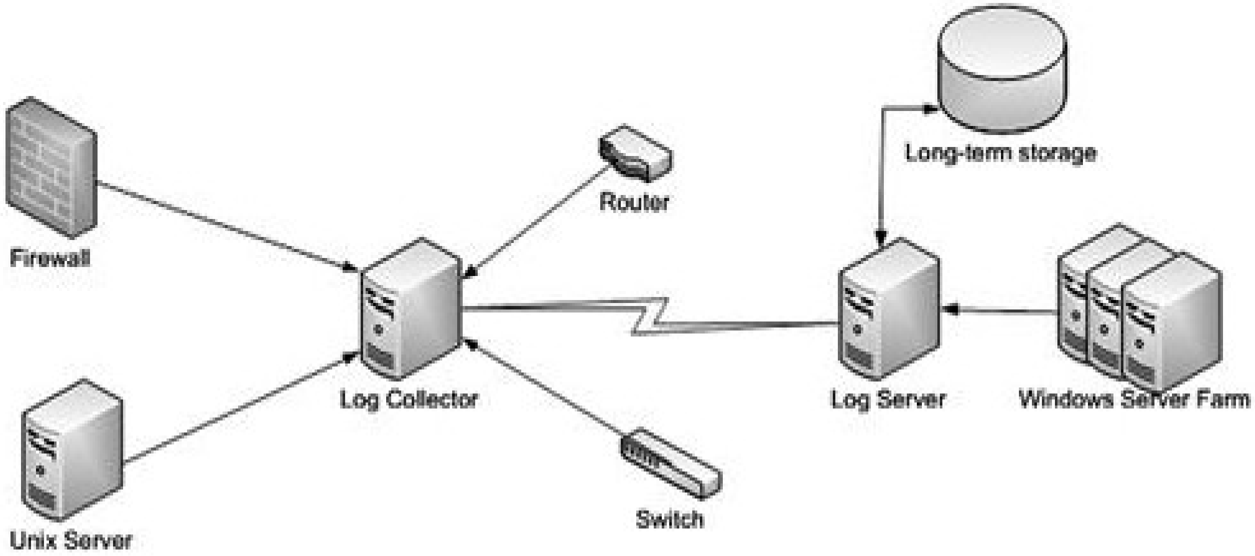


- Single log server which has several devices sending logs to it – simplest

Log server and log collector deployment



- Distribute log collectors in strategic points in your network – more common deployment model
- The log server acts as the central place for reviewing logs, analysing logs
- The log collectors only backs up your logs temporarily



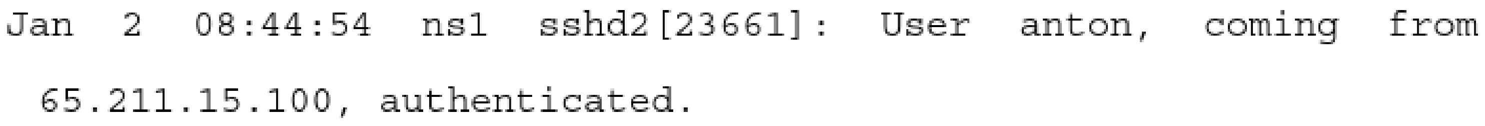
Log server and log collector with long-term storage

Logging policy on data collection

- A log message should tell what happened and why it happened
- *State*
  - Program variable, return values
  - Stack information
- *Context*
  - Supporting information, describing why the log message is written

OS logs

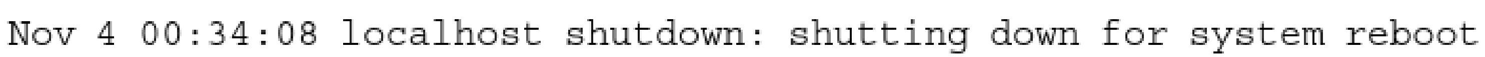
- Authentication



```
Jan  2  08:44:54  ns1  sshd2[23661]:  User  anton,  coming  from
 65.211.15.100, authenticated.
```

  - Linux syslog, remote user authenticating with Secure Shell (SSH) daemon

- Sy

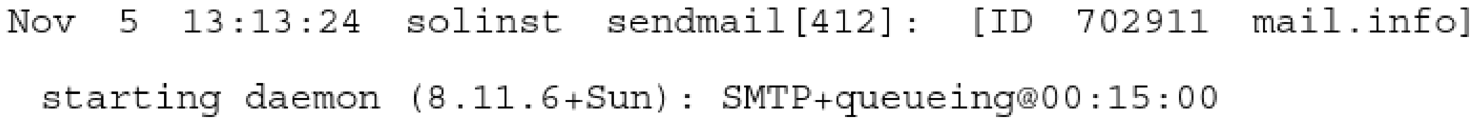


```
Nov 4 00:34:08 localhost shutdown: shutting down for system reboot
```

  - Linux syslog, system shutdown

OS logs

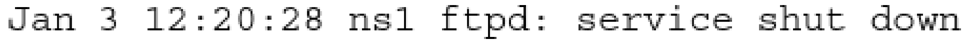
- Service startup, shutdown and status change



```
Nov  5  13:13:24  solinst  sendmail[412]:  [ID  702911  mail.info]
 starting daemon (8.11.6+Sun): SMTP+queueing@00:15:00
```

  - Solaris syslog, sendmail daemon starts up

- Service crash

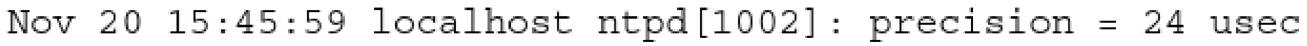


```
Jan 3 12:20:28 ns1 ftpd: service shut down
```

  - Linux syslog, FYP server shutting down involuntarily (due to a crash or a kill command)

OS logs

- Miscellaneous status message



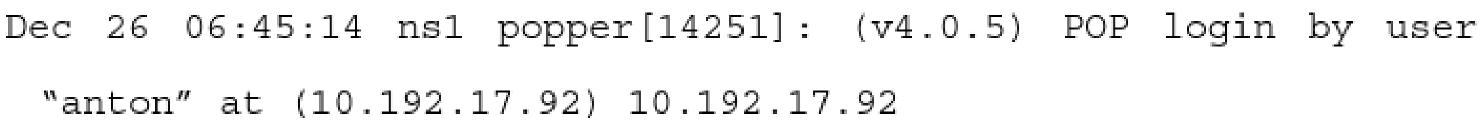
```
Nov 20 15:45:59 localhost ntpd[1002]: precision = 24 usec
```

  - Linux syslog of a time synchronization daemon (NTPD)

- OS logs are security relevant
  - Useful for intrusion detection
  - Useful for incident response

Network daemon logs

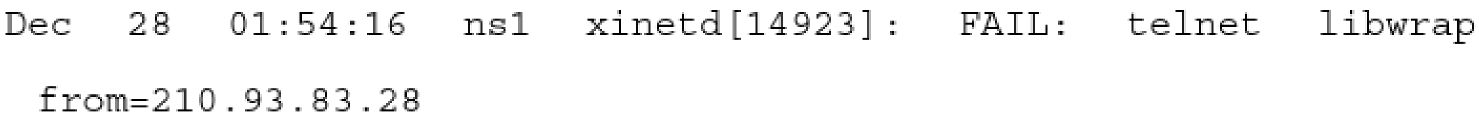
- Connection established to the service



```
Dec 26 06:45:14 ns1 popper[14251]: (v4.0.5) POP login by user
 "anton" at (10.192.17.92) 10.192.17.92
```

  - remote user “anton”

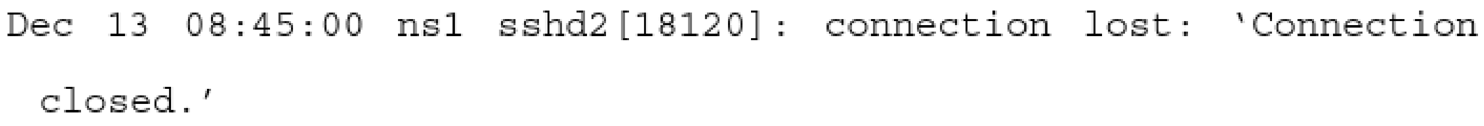
- Connection failed to server



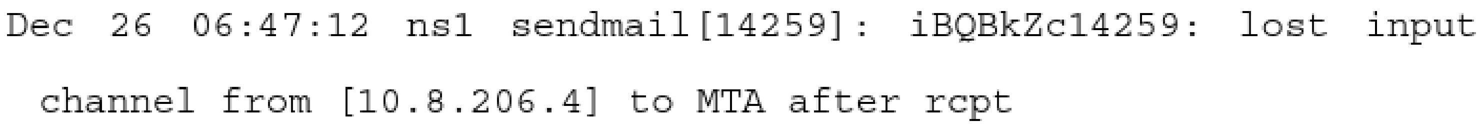
```
Dec  28  01:54:16  ns1  xinetd[14923]:  FAIL:  telnet  libwrap
 from=210.93.83.28
```

  - Linux syslog shows a connection failure (due to access controls) to a telnet service

Network daemon logs

- Connection was established, but access was not allowed
  - 

```
Dec 13 08:45:00 ns1 sshd2[18120]: connection lost: 'Connection
 closed.'
```

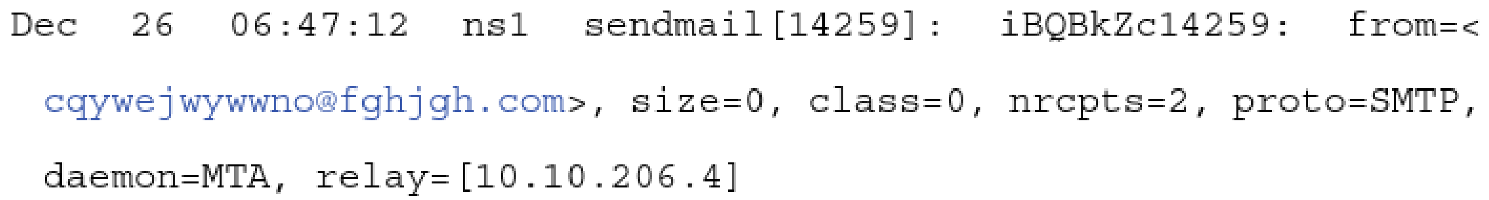
- Various failure messages
  - 

```
Dec 26 06:47:12 ns1 sendmail[14259]: iBQBkZc14259: lost input
 channel from [10.8.206.4] to MTA after rcpt
```

  - Linux syslog message shows a failure of a sendmail daemon to continue talking to a client (likely a spam program)

Network daemon logs

- Various status messages



```
Dec  26  06:47:12  ns1  sendmail[14259]:  iBQBkZc14259:  from=<
 cqywejwywwno@fghjgh.com>, size=0, class=0, nrcpts=2, proto=SMTP,
 daemon=MTA, relay=[10.10.206.4]
```

  - Linux syslog message indicates a successful Email transfer

- Network daemons present the most common entryways into the system remotely and many of the attacks are targeted against them

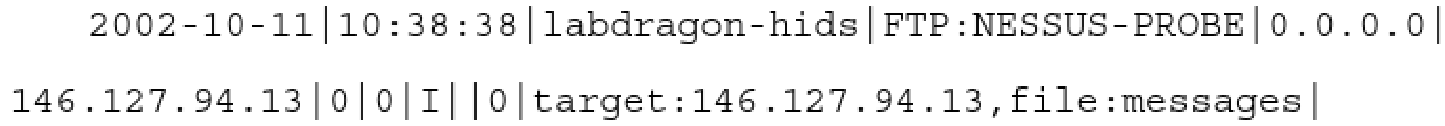
Application logs

Types of application logs

- Application user activity
- Privileged user activity
- Routine but critical activity
- Reconfiguration

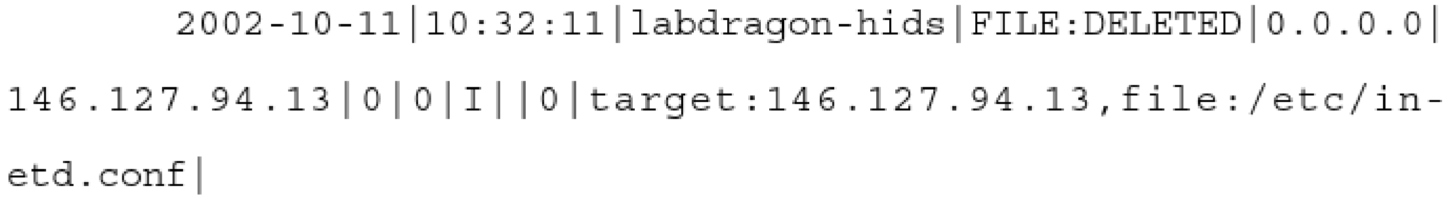
HIDS & HIPS

- Dragon HIDS examples
  - A Nessus vulnerability scanner probe is detected by watching the FTP log



```
    2002-10-11|10:38:38|labdragon-hids|FTP:NESSUS-PROBE|0.0.0.0|
146.127.94.13|0|0|I||0|target:146.127.94.13,file:messages|
```

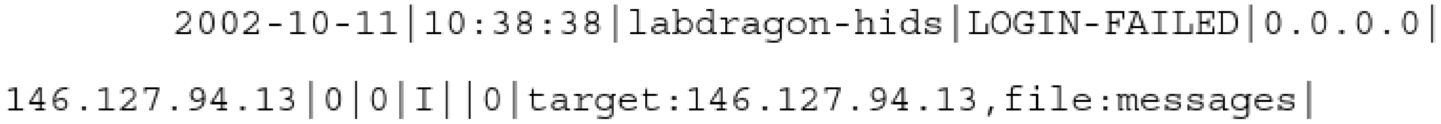
  - Insecure system reconfiguration or corruption
  -



```
      2002-10-11|10:32:11|labdragon-hids|FILE:DELETED|0.0.0.0|
146.127.94.13|0|0|I||0|target:146.127.94.13,file:/etc/in-
etd.conf|
```

HIDS & HIPS

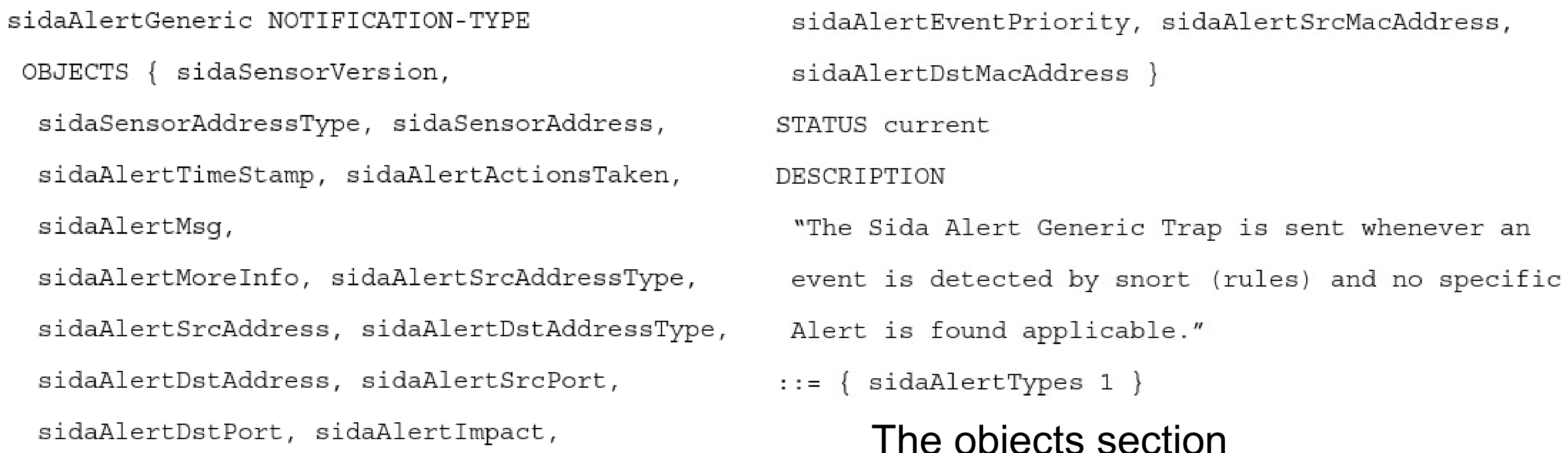
- Authentication or authorization failed



```
          2002-10-11|10:38:38|labdragon-hids|LOGIN-FAILED|0.0.0.0|
146.127.94.13|0|0|I||0|target:146.127.94.13,file:messages|
```

Common log source protocols -- SNMP traps/notifications

- Example notification from Snort MIB

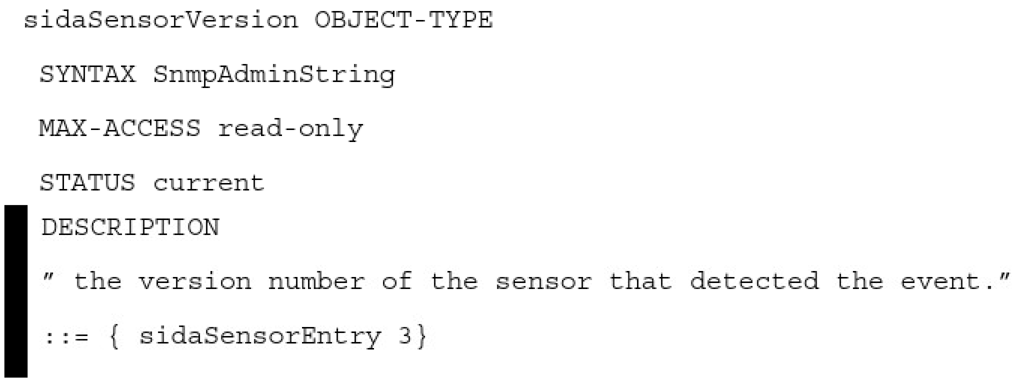


```
sidaAlertGeneric NOTIFICATION-TYPE
 OBJECTS { sidaSensorVersion,
  sidaSensorAddressType, sidaSensorAddress,
  sidaAlertTimeStamp, sidaAlertActionsTaken,
  sidaAlertMsg,
  sidaAlertMoreInfo, sidaAlertSrcAddressType,
  sidaAlertSrcAddress, sidaAlertDstAddressType,
  sidaAlertDstAddress, sidaAlertSrcPort,
  sidaAlertDstPort, sidaAlertImpact,
  sidaAlertEventPriority, sidaAlertSrcMacAddress,
  sidaAlertDstMacAddress }
 STATUS current
 DESCRIPTION
  "The Sida Alert Generic Trap is sent whenever an
  event is detected by snort (rules) and no specific
  Alert is found applicable."
 ::= { sidaAlertTypes 1 }
```

The objects section contains individual event details

Common log source protocols -- SNMP traps/notifications

- sideSensorVersion is defined in the same MIB



```
sidaSensorVersion OBJECT-TYPE
 SYNTAX SnmpAdminString
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 " the version number of the sensor that detected the event."
 ::= { sidaSensorEntry 3}
```

- It’s a string representing the version of Snort that reported the notification

Common log source protocols -- SNMP traps/notifications

- Vendors rarely provide well formatted understandable messages
  - MIB may not match up with the actual trap or notification sent by the device or system
  - MIB is out of sync with changes in the underlying SNMP implementation
  - Many vendors create a trap that sends a single variable as a free-form text
    - take the exact message they would send as a Syslog message and warp it in an SNMP trap

Log rotation

Log rotation

- an active log file is moved to an archive copy, and
- a new empty file is created for an application to begin writing to

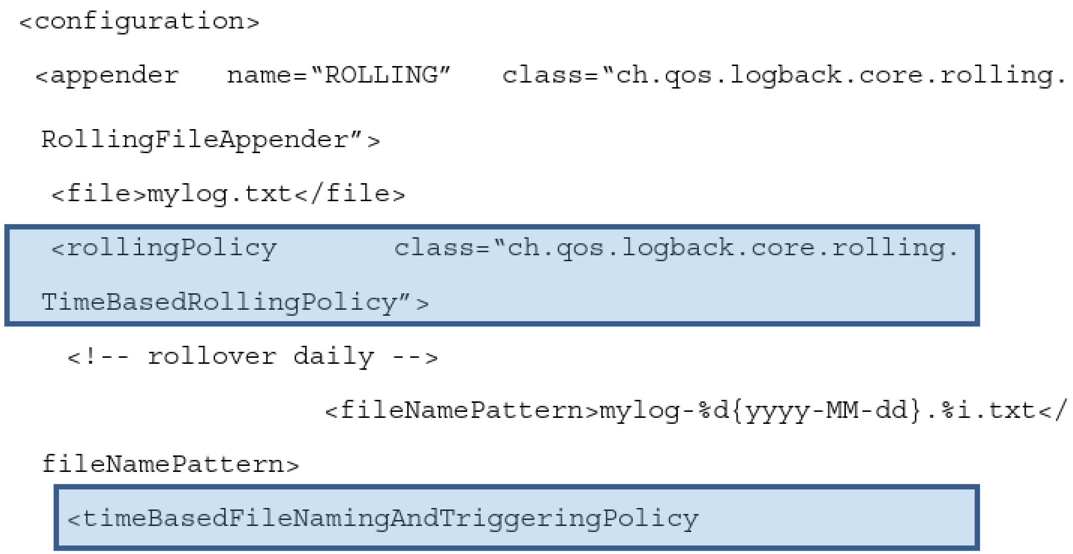
2 basic types of mechanisms

- Log rotation scripts
- The application itself handles log rotation duties
  - Handled by custom-written application code
  - Built-in features of a third-party logging library
- Application does not need to know that log rotation has occurred

Log rotation schemes

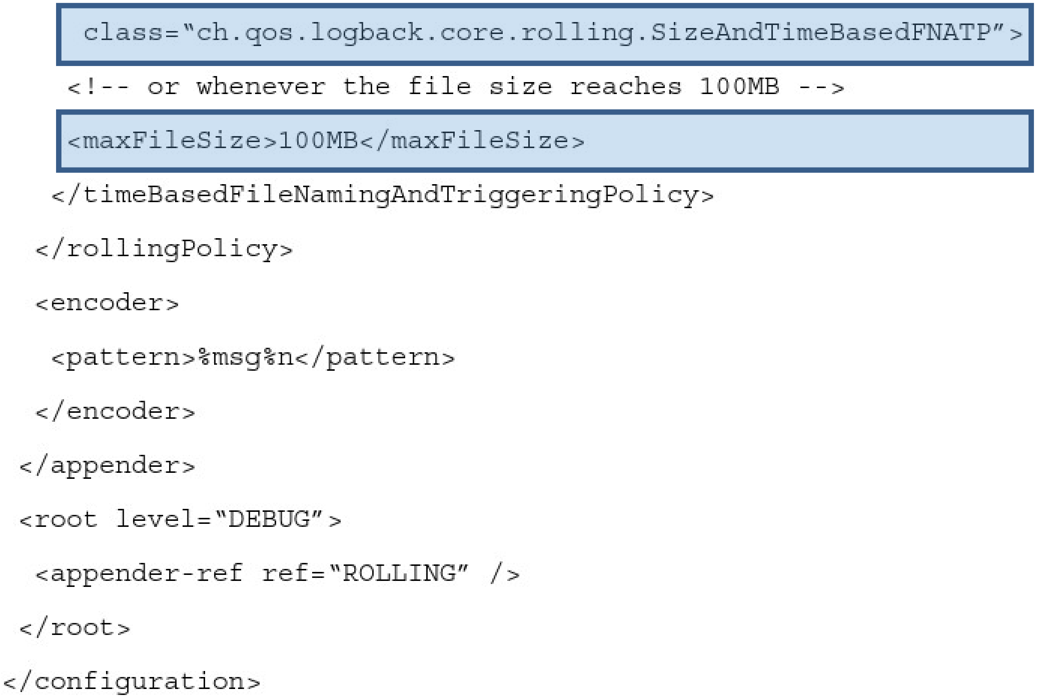
- Time based
  - Hourly, daily, weekly, etc
- Size based
  - 10 MB, 10 MB, etc
- Size and time based
  - Log file is archived based on time but each log file is also capped at some size

Logback example on log rotation



```
<configuration>
 <appender   name="ROLLING"   class="ch.qos.logback.core.rolling.
 RollingFileAppender">
  <file>mylog.txt</file>
  <rollingPolicy       class="ch.qos.logback.core.rolling.
 TimeBasedRollingPolicy">
   <!-- rollover daily -->
                   <fileNamePattern>mylog-%d{yyyy-MM-dd}.%i.txt</
 fileNamePattern>
   <timeBasedFileNamingAndTriggeringPolicy
```

Logback example on log rotation (con’d)



```
   class="ch.qos.logback.core.rolling.SizeAndTimeBasedFNATP">
  <!-- or whenever the file size reaches 100MB -->
  <maxFileSize>100MB</maxFileSize>
 </timeBasedFileNamingAndTriggeringPolicy>
</rollingPolicy>
<encoder>
 <pattern>%msg%n</pattern>
</encoder>
</appender>
<root level="DEBUG">
 <appender-ref ref="ROLLING" />
</root>
</configuration>
```

- Rotate the log file each day *OR* when it reaches 100 MB
  - Manageable chunk of log data

Logging policy on log retention / storage

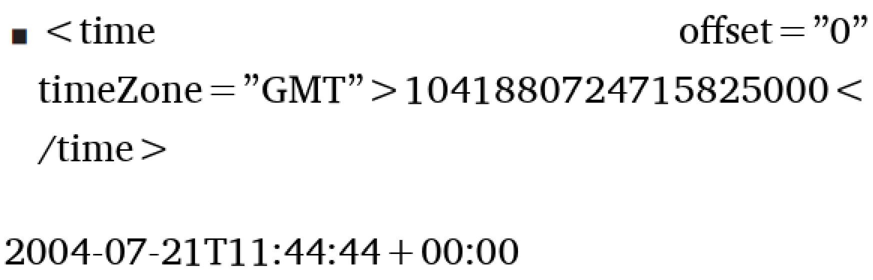
- Retention / storage
  - Log storage, accessibility and log destruction
  - Never use a syslog server as a log retention system
  - Storage size per day:
  - Log records (in bytes) per second * 86400 seconds
  - General rule of thumb is to add 25% to your log retention capacity needs
  - Distributed storage

High level concerns on planning

- Accuracy – free from defects or misleading information
  - Reduce false positives, e.g.
  - IDS to consult a vulnerability database
  - IDS to implement a policy scheme whereby user and group profiles are used to create acceptable network usage of individuals

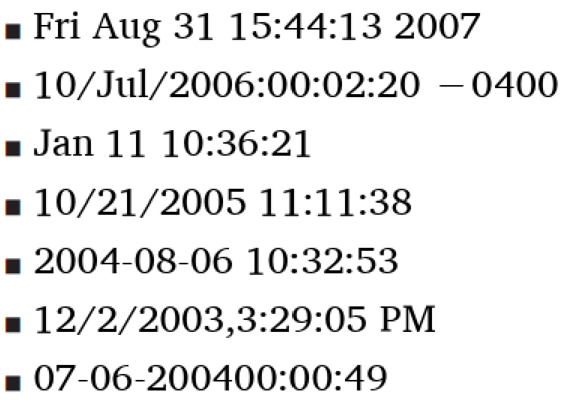
High level concerns on planning

- Accuracy – free from defects or misleading information (cont’d)
  - Timestamp
  - Different vendors use different formats
  - e.g.



- <time offset=”0” timeZone=”GMT”>1041880724715825000</time>

2004-07-21T11:44:44+00:00



- Fri Aug 31 15:44:13 2007
- 10/Jul/2006:00:02:20 –0400
- Jan 11 10:36:21
- 10/21/2005 11:11:38
- 2004-08-06 10:32:53
- 12/2/2003,3:29:05 PM
- 07-06-200400:00:49

  - ISO 8601 standard
  - YYYY-MM-DDTHH:MM:SS.SSS +/-H

High level concerns on planning

- Integrity
  - Authenticate client and server, encrypt data
  - Send data in clear, but use dedicated network
  - Digital signature

- Confidence
  - Priority or severity
  - E.g. cisco devices use a scale from 0 through 7
  - Take input from many disjoint areas, and deriving a more mature and accurate fact from the set of all inputs

High level concerns on planning

- Preservation
- Sanitization
  - Remove or replace the attributes you want sanitized
    - IP address becomes xxx.xxx.xxx.xxx
  - Sanitized log data is extracted and placed into a secure file, can be reconstructed at some later point
- Normalization – translate to a well known log event format
- Challenges with time synchronization

www.sp.edu.sg

Singapore Polytechnic
500 Dover Road
Singapore 139651

tel. (65) 6775 1133
fax. (65) 6870 6189