第 5 章

日 志 分 析

健全的日志记录和分析系统是系统正常运营与优化以及安全事故响应的基础，虽然安全系统供应商为我们提供了五花八门的解决方案，但是最终的基础仍是具有充足性、可用性、安全性的日志记录系统。作为运维人员，以及为企业开发应用程序的开发人员，能不能回答上述问题，正是对我们实际工作能力的一个考验。

在实际工作中可以看到，许多单位内部对日志并没有充分的认识，安全工作更多地投入设备，比如防火墙、IDS、IPS、防病毒软件等，被动地希望这些系统帮助我们完成一切工作，但是俗话说得好“道高一尺，魔高一丈”，以特征码和预定义规则为基础的上述设备，在防护方面永远落在攻击者的后面，防微杜渐才是真正的出路。作为一名合格的运维人员，了解日志的概念，了解日志的配置和分析方法，是发现威胁、抵御攻击的重要技能，有了这方面的深刻认识，各种自动化安全解决方案才能真正地发挥效能。

5.1 日志分析介绍

日志就是按照一定的规则将操作系统、应用程序、网络设备中发生的事件记录下来，对系统管理、网络安全策略实施状况的评估及其他安全防御系统的评估都是必不可少的证据。因此，日志成为系统的调试和管理等日常维护中不可或缺的工具，起到预防和阻止网络犯罪的作用。

5.1.1 日志文件的特点及日志分析的目的

1. 日志文件的特点

系统中特定时间的活动信息都被记录在日志中，通过对日志进行分析，总结了如下几个主要特点。

1）多样性

操作系统、服务、网络设备及应用软件的不同使得日志在格式和存储方式上存在较大的差异，并且记录的内容和侧重点不同，同时由于国内外没有关于日志的统一标准和格式，导致系统日志的统一处理更加困难。

2）可读性差

大多数计算机系统日志是以二进制形式存储的，并且各个系统日志格式不一致，使得获取有用信息十分困难。日志记录的具体含义需要借助相应的帮助和说明文档才能明白，导致普通非计算机系统管理人员对通过日志获取系统信息变得捉襟见肘。

3）日志记录的数据量很大

计算机系统日志记录了诸如 Web 服务器、数据库日志、防火墙日志以及系统中关于进程及文件等所有的信息，产生的大量日志数据使得其存储和分析存在较大的困难，更不必说通过人工阅读和分析日志文件来实时发现计算机安全事件。

4）不容易获取

各系统开发商和网络设备生产商常根据各自的需要来设定日志的格式，提供的接口也是差异较大，使得产生的日志在格式和存储方式上各不相同，同时日志会随着系统运行状态的变化而变化，致使日志的获取更加困难。

5）不同日志之间存在某种必然的联系

一个系统事件可能被记录在多个系统日志中，例如，一个用户的网络活动会在操作系统日志、防火墙日志、IDS 日志等系统日志中留下痕迹，只有将这些相关日志综合起来分析，才能准确地获取该用户的活动意图及活动情况。

6）容易被篡改

计算机系统日志存在较大的安全隐患，没有加密校验和防止恶意篡改的有效保护机制，并以文本的形式存储在未经保护的目录中，一方面系统日志的产生和保存方式可以通过修改注册表和 syslog 的配置文件进行修改或停止日志进程，另一方面可以通过修改、删除或伪造来误导网络管理员获取不实信息。因此，日志文件不一定是可靠的，从而不能视为有效的证据。

2. 日志分析目的

日志作为计算机系统的辅助管理工具，主要应用表现在以下几个方面。

（1）对用户行为进行审计。系统日志通过监控账户使用情况及用户的行为来防止行为的滥用。

（2）监控恶意行为。日志能够反映非法用户在网络系统中的各种恶意行为，通过日志可以有效监控恶意用户的行为，检测不合法行为。

(3) 对入侵行为的检测。通过及时收集、保全和分析不安全策略的行为及系统和网络行为的原始信息对黑客入侵系统的线路进行追踪。

(4) 系统资源的监控。获得计算机系统中内存、硬盘、进程、网络、文件、外围设备等的使用情况,并发现资源的异常占用及磁盘等硬件资源错误。

(5) 帮助恢复系统。系统遭到破坏前的状态信息以及入侵过程和结果信息都被记录在系统日志中,可以帮助迅速定位系统故障原因,进而恢复系统功能。

(6) 评估造成的损失。可以确定入侵行为的范围并进一步评估损失,以便采取相应的应对措施。

(7) 计算机犯罪的取证。记录系统和网络行为的原始信息,通过及时收集、管理和分析系统日志,可以帮助追踪攻击者入侵网络系统的路径,对计算机犯罪活动进行取证,从而打击和震慑计算机犯罪活动。

(8) 调查报告的生成。可以根据日志获取的入侵工具、过程、结果以及攻击者的身份获得详尽的调查报告。

然而,由于日志不仅数据海量,格式和存储方式不统一,而且不同日志间有联系,使得对日志的分析变得更加困难。如果网络管理员能够明白这些信息的意思,更为重要的是知道如何分析和使用这些信息,那么日志用于网络安全管理的价值将无法估量。

5.1.2 日志的分类

网络环境中存在着各种各样的日志,从不同的角度看有不同的分类。从日志产生的来源角度分类,日志主要分为三大类:操作系统日志(UNIX/Linux,Windows 等)、网络设备日志(路由交换设备、防火墙等安全设备)、应用服务日志(Web 等各种网络应用)[1]。

1. UNIX/Linux 系统日志

UNIX/Linux 的系统日志能细分为以下三个日志子系统。

(1) 登录时间日志子系统:登录时间日志通常会与多个程序的执行产生关联,一般情况下,将对应的记录写到/var/log/wtmp 和/var/run/utmp 中。为了使系统管理员能够有效地跟踪谁在何时登录过系统,一旦触发 login 等程序,就会对 wtmp 和 utmp 文件进行相应的更新。

(2) 进程统计日志子系统:主要由系统的内核来实现完成记录操作。如果一个进程终止,系统就能够自动记录该进程,并在进程统计的日志文件中添加相应的记录。该类日志能够记录系统中各个基本的服务,可以有效地记录与提供相应命令在某一系统中使用的详细统计情况。

(3) 错误日志子系统:其主要由系统进程 syslogd(新版 Linux 发行版采用 rsyslogd 服

务)实现操作。它由各个应用系统(例如 Http、Ftp、Samba 等)的守护进程、系统内核来自动利用 syslog 向/var/log/messages 文件中进行记录添加,用来向用户报告不同级别的事件。

Linux 系统日志如图 5.1 所示。

```
Nov 24 00:23:36 zjd-virtual-machine AptDaemon: INFO: Quitting was requested
Nov 24 00:24:05 zjd-virtual-machine anacron[1136]: Job 'cron.daily' terminated
Nov 24 00:25:49 zjd-virtual-machine kernel: [  604.692962] pcnet32 0000:02:01.0 eth0: link up
Nov 24 00:25:49 zjd-virtual-machine kernel: [  604.693073] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> (eth0): carrier now ON (device state 20)
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> (eth0): device state change: unavailable -> disconnected (reason 'carrier-changed') [20 30 46
Nov 24 00:25:51 zjd-virtual-machine avahi-daemon[966]: Joining mDNS multicast group on interface eth0.IPv6 with address fe80::20c:29ff:fe0e:e8ba.
Nov 24 00:25:51 zjd-virtual-machine avahi-daemon[966]: New relevant interface eth0.IPv6 for mDNS.
Nov 24 00:25:51 zjd-virtual-machine avahi-daemon[966]: Registering new address record for fe80::20c:29ff:fe0e:e8ba on eth0.*.
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> Auto-activating connection 'Wired connection '.
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> Activation (eth0) starting connection 'Wired connection '
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> (eth0): device state change: disconnected -> prepare (reason 'none') [30 40 0]
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> Activation (eth0) Stage 1 of 5 (Device Prepare) scheduled...
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> Activation (eth0) Stage 1 of 5 (Device Prepare) started...
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> Activation (eth0) Stage 2 of 5 (Device Configure) scheduled...
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> Activation (eth0) Stage 1 of 5 (Device Prepare) complete.
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> Activation (eth0) Stage 2 of 5 (Device Configure) starting...
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> (eth0): device state change: prepare -> config (reason 'none') [40 50 0]
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> Activation (eth0) Stage 2 of 5 (Device Configure) successful.
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> Activation (eth0) Stage 3 of 5 (IP Configure Start) scheduled.
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> Activation (eth0) Stage 2 of 5 (Device Configure) complete.
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> Activation (eth0) Stage 3 of 5 (IP Configure Start) started...
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> (eth0): device state change: config -> ip-config (reason 'none') [50 70 0]
Nov 24 00:25:51 zjd-virtual-machine NetworkManager[1005]: <info> Activation (eth0) Beginning DHCPv4 transaction (timeout in 45 seconds)
Nov 24 00:25:52 zjd-virtual-machine NetworkManager[1005]: <info> dhclient started with pid 3326
Nov 24 00:25:52 zjd-virtual-machine dhclient: Internet Systems Consortium DHCP Client 4.1-ESV-R4
Nov 24 00:25:52 zjd-virtual-machine dhclient: Copyright 2004-2011 Internet Systems Consortium.
Nov 24 00:25:52 zjd-virtual-machine dhclient: All rights reserved.
Nov 24 00:25:52 zjd-virtual-machine dhclient: For info, please visit https://www.isc.org/software/dhcp/
```

图 5.1　Linux 系统日志

2. Windows 系统日志

Windows 的日志文件主要包括:系统日志、安全日志、应用程序日志、安装日志及转发日志。可以通过 Windows 的事件查看器查看相关日志。

(1) 系统日志。主要是指 Windows 2008、Windows 7 等各种操作系统中的各个组件在运行中产生的各种事件。这些事件一般可以分为:系统中各种驱动程序在运行中出现的重大问题、操作系统的多种组件在运行中出现的重大问题以及应用软件在运行中出现的重大问题等,而这些重大问题主要包括重要数据的丢失、错误等,甚至是系统产生的崩溃行为。如图 5.2 所示为 Windows 7 系统日志。

级别	日期和时间	来源	事件 ID	任务类别
信息	02/11/2015 08:59:08	Service Control Manager	7036	无
信息	02/11/2015 08:54:06	Service Control Manager	7036	无
信息	02/11/2015 08:50:29	Service Control Manager	7036	无
信息	02/11/2015 08:48:58	Service Control Manager	7036	无
信息	02/11/2015 08:46:45	Service Control Manager	7036	无
信息	02/11/2015 08:39:48	Service Control Manager	7036	无
信息	02/11/2015 08:35:11	Service Control Manager	7036	无
信息	02/11/2015 08:34:27	Service Control Manager	7036	无
信息	02/11/2015 08:34:07	Service Control Manager	7036	无
信息	02/11/2015 08:33:56	Service Control Manager	7036	无

图 5.2　Windows 7 系统日志

(2) 安全日志。Windows 安全日志与系统日志明显不同,主要记录各种与安全相关的事件。构成该日志的内容主要包括:各种对系统进行登录与退出的成功或者不成功信息;对系统中的各种重要资源进行的各种操作(比如:对系统文件进行创建、删除、更改等不同的操作)。如图 5.3 所示为 Windows 7 安全日志。

级别	日期和时间	来源	事件 ID	任务类别
信息	02/11/2015 08:31:54	Microsoft Windows 安全审核。	4672	特殊登录
信息	02/11/2015 08:31:54	Microsoft Windows 安全审核。	4624	登录
信息	02/11/2015 08:31:54	Microsoft Windows 安全审核。	4648	登录
信息	02/11/2015 08:30:47	Microsoft Windows 安全审核。	4624	登录
信息	02/11/2015 08:30:34	Microsoft Windows 安全审核。	4672	特殊登录
信息	02/11/2015 08:30:34	Microsoft Windows 安全审核。	4624	登录
信息	02/11/2015 08:30:23	Microsoft Windows 安全审核。	4672	特殊登录
信息	02/11/2015 08:30:23	Microsoft Windows 安全审核。	4624	登录
信息	02/11/2015 08:30:19	Microsoft Windows 安全审核。	5056	系统完整性
信息	02/11/2015 08:30:17	Microsoft Windows 安全审核。	4672	特殊登录
信息	02/11/2015 08:30:17	Microsoft Windows 安全审核。	4624	登录

图 5.3 Windows 7 安全日志

(3) 应用程序日志。它主要记录各种应用程序所产生的各类事件。比如,系统中 SQL Server 数据库程序进行备份设定,一旦成功完成数据的备份操作,就立即向指定的日志发送记录,该记录中包含与对应的事件相关的详细信息。如图 5.4 所示为 Windows 7 应用程序日志。

级别	日期和时间	来源	事件 ID	任务类别
信息	02/11/2015 08:39:48	Security-SPP	903	无
信息	02/11/2015 08:38:01	Ci	4137	CI 服务
信息	02/11/2015 08:37:27	LoadPerf	1000	无
信息	02/11/2015 08:37:27	LoadPerf	1001	无
信息	02/11/2015 08:34:48	Security-SPP	902	无
信息	02/11/2015 08:34:48	Security-SPP	1003	无
信息	02/11/2015 08:34:47	Security-SPP	1066	无
信息	02/11/2015 08:34:28	SecurityCenter	1	无
信息	02/11/2015 08:34:06	Security-SPP	900	无
信息	02/11/2015 08:33:28	LMS	2000	LMS
信息	02/11/2015 08:33:05	IntelDalJhi	0	无

图 5-4 Windows 7 应用程序日志

3. 网络设备日志

通常网络设备包括路由交换设备、防火墙、入侵检测及 UPS 系统等。由于上述设备的厂家和标准差异,它们在产生日志时,必然存在着不同的格式。下面以防火墙、交换机和路由器举例说明。

1) PIX 防火墙日志

该日志是与实际的防火墙系统产品相关的。其主要由 Cisco 公司进行研发,该防火墙主要基于专用操作系统,同时采取实时的嵌入式系统来形成支撑。PIX 系列的防火墙通常

都为用户提供了比较完备的安全审计方法，其主要记录的事件如下。

（1）AAA（认证、授权和记账）事件。

（2）Connection（连接）事件。

（3）SNMP 事件。

（4）Routing errors（路由错误）事件。

（5）Failover（故障转移）事件。

（6）PIX 系统管理事件。

如图 5.5 所示为防火墙日志。

```
[06/16/11 13:16:37] ufw allow in proto tcp from 192.168.0.100 port 22 to 192
[06/16/11 13:16:53] ufw --force delete 1
[06/16/11 13:17:41] ufw allow in log-all proto tcp from 192.168.0.100 port 22
[06/16/11 13:18:37] ufw allow in log-all proto tcp from 192.168.0.105 port 22
[06/16/11 13:18:46] ufw --force delete 1
[06/16/11 13:19:14] ufw default allow incoming
[06/16/11 13:19:29] ufw default reject incoming
[06/16/11 13:19:55] ufw --force delete 1
[06/16/11 13:20:16] ufw allow in proto tcp from 192.168.0.1 port 22 to 192.1
[06/16/11 13:23:15] ufw --force delete 1
[06/16/11 13:23:42] ufw allow in proto tcp from 192.168.0.105 port 22 to any
[06/16/11 13:27:06] ufw --force delete 1
[06/16/11 13:27:19] ufw allow in proto tcp from 192.168.0.105 port 22 to any
[06/16/11 13:27:42] ufw allow in proto tcp from 192.168.0.105/24 port 22 to
[06/16/11 13:27:47] ufw --force delete 1
[06/16/11 13:31:26] ufw allow in from 192.168.0.105/24 port 22 to any port 2
[06/16/11 13:31:50] ufw --force delete 1
[06/16/11 13:31:56] ufw --force delete 1
[06/16/11 13:32:00] ufw --force delete 1
[06/16/11 13:32:42] ufw allow in from 192.168.0.0/24 port 22 to any port 22
```

图 5.5　防火墙日志

2）交换机日志

中高端交换机以及各种路由器，一般情况下都会采取一定的方式记录设备自身的运行状态，并且将系统在运行中产生的一些异常情况记录下来。另外，在兼容性方面，上述网络设备通常都提供了对 Syslog RFC 3164 的支持，并对该协议所明确的各种日志处理机制提供支持，因此可以通过 Syslog 协议来实现不同设备之间多种日志的相互转发。如图 5.6 所示为交换机日志。

```
<date> <time> <facility>.<severity> <program[<pid>]>: <message>
-------------------------------------------------------------------------------
2011 Nov 15 14:39:04 user.information awplus system: Warm Boot....
2011 Nov 15 14:39:04 user.information awplus evlog: Event log initialized
2011 Nov 15 14:39:04 user.information awplus file: File System initialized
2011 Nov 15 14:39:04 user.information awplus ssh: SSH server disabled
.....
```

图 5.6　交换机日志

3）路由器日志

如图 5.7 所示为路由器日志。

```
1 Mar 26 10:47:24.955 VTTY: Console port: waiting connection on tcp port 5000
  1 (FD 10)
2 Mar 26 10:47:26.073 C3600_BOOT: starting instance (CPU0 PC=0xffffffffbfc000
  00,idle_pc=0x0,JIT on)
3 Mar 26 10:47:26.074 CPU0: CPU_STATE: Starting CPU (old state=2)...
4 Mar 26 10:47:26.197 ROM: Microcode has started.
5 Mar 26 10:47:37.620 ROM: trying to read bootvar 'NO_CP0'
6 Mar 26 10:47:37.620 ROM: trying to read bootvar 'NO_RANDOM_NUM'
7 Mar 26 10:47:37.620 ROM: trying to read bootvar 'RANDOM_NUM'
8 Mar 26 10:47:37.620 ROM: trying to read bootvar 'OFFSET'
9 Mar 26 10:47:40.975 CPU0: IO_FPGA: write to unknown addr 0x30006, value=0x0
  , pc=0x60698844 (size=1)
10 Mar 26 10:47:40.985 CPU0: IO_FPGA: write to unknown addr 0x30006, value=0x0
  , pc=0x60698844 (size=1)
11 Mar 26 10:47:40.996 CPU0: IO_FPGA: write to unknown addr 0x30006, value=0x0
  , pc=0x60698844 (size=1)
12 Mar 26 10:47:41.007 CPU0: IO_FPGA: write to unknown addr 0x30006, value=0x0
  , pc=0x60698844 (size=1)
13 Mar 26 10:47:41.009 ROM: unhandled syscall 0x00000047 at pc=0x605ecfb8 (a1=
  0x6293b590,a2=0x00000000,a3=0x00000000)
14 Mar 26 10:47:41.203 ROM: trying to read bootvar 'RANDOM_NUM'
```

图 5.7　路由器日志

4. 应用系统日志

应用系统的日志是指在系统的工作过程中，对应用程序的某些重要事件进行记录形成的日志，例如 Apache、FTP、Samba、NFS、DHCP、NFS 及微软 IIS 日志等。

常用应用程序日志举例如下。

Apache 服务器的日志如图 5.8 所示。

```
::1 - - [23/Mar/2014:15:07:00 -0700] "GET /images/apache_feather.gif HTTP/1.1" 200 4128
::1 - - [23/Mar/2014:15:07:04 -0700] "GET /images/producer_consumer.png HTTP/1.1" 200 8
::1 - - [23/Mar/2014:15:07:04 -0700] "GET /images/log_anatomy.png HTTP/1.1" 200 19579
::1 - - [23/Mar/2014:15:07:04 -0700] "GET /images/consumer-groups.png HTTP/1.1" 200 268
::1 - - [23/Mar/2014:15:07:04 -0700] "GET /images/log_compaction.png HTTP/1.1" 200 4141
::1 - - [23/Mar/2014:15:07:04 -0700] "GET /documentation.html HTTP/1.1" 200 189893
::1 - - [23/Mar/2014:15:07:04 -0700] "GET /images/log_cleaner_anatomy.png HTTP/1.1" 200
::1 - - [23/Mar/2014:15:07:04 -0700] "GET /images/kafka_log.png HTTP/1.1" 200 134321
::1 - - [23/Mar/2014:15:07:04 -0700] "GET /images/mirror-maker.png HTTP/1.1" 200 17054
::1 - - [23/Mar/2014:15:08:07 -0700] "GET /documentation.html HTTP/1.1" 200 189937
::1 - - [23/Mar/2014:15:08:07 -0700] "GET /styles.css HTTP/1.1" 304 -
::1 - - [23/Mar/2014:15:08:07 -0700] "GET /images/kafka_logo.png HTTP/1.1" 304 -
::1 - - [23/Mar/2014:15:08:07 -0700] "GET /images/producer_consumer.png HTTP/1.1" 304 -
::1 - - [23/Mar/2014:15:08:07 -0700] "GET /images/log_anatomy.png HTTP/1.1" 304 -
::1 - - [23/Mar/2014:15:08:07 -0700] "GET /images/consumer-groups.png HTTP/1.1" 304 -
::1 - - [23/Mar/2014:15:08:07 -0700] "GET /images/log_cleaner_anatomy.png HTTP/1.1" 304
::1 - - [23/Mar/2014:15:08:07 -0700] "GET /images/log_compaction.png HTTP/1.1" 304 -
::1 - - [23/Mar/2014:15:08:07 -0700] "GET /images/kafka_log.png HTTP/1.1" 304 -
::1 - - [23/Mar/2014:15:08:07 -0700] "GET /images/mirror-maker.png HTTP/1.1" 304 -
::1 - - [23/Mar/2014:15:09:55 -0700] "GET /documentation.html HTTP/1.1" 200 195264
```

图 5.8　Apache 服务器日志

FTP 服务器的日志如图 5.9 所示。

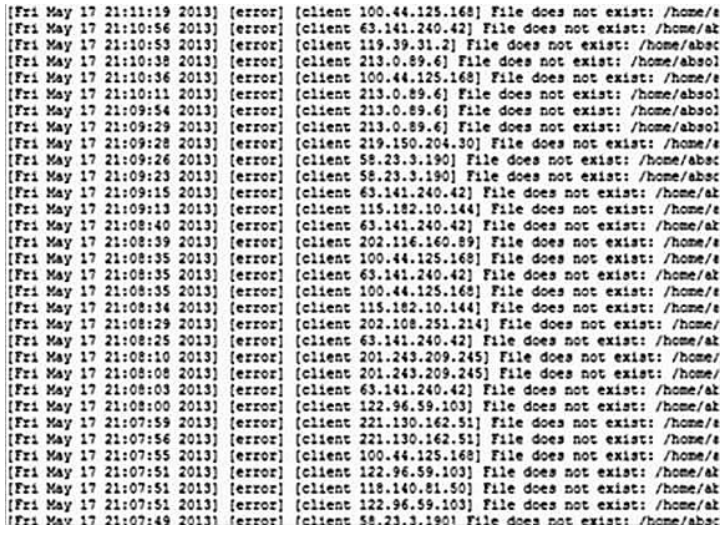

图 5.9　FTP 服务器错误日志

5.1.3　网络日志分析相关术语

日志分析产品：通过日志代理、标准协议、文件导入等方式采集信息系统中的日志数据，并进行集中存储和分析的安全产品。

日志数据源：产生日志数据的原始来源[2]。

日志管理中心：对采集到的日志数据进行集中处理、存储、分析的功能模块。

审计日志：日志分析产品自身审计产生的日志数据。

日志记录：对采集到的原始日志数据进行预处理之后，根据一定规则生成并保存在日志管理中心的日志数据。

授权管理员：具有日志分析产品管理权限的用户，负责对日志分析产品的系统配置、安全策略和日志数据进行管理。

可信主机：赋予权限能够管理日志分析产品的主机。

日志分析产品应能对日志数据源进行添加、修改和删除等管理操作，并且日志数据源的类型应至少包含以下范围。

（1）网络设备，如交换机、路由器、防火墙等；

（2）操作系统；

（3）数据库系统；

（4）其他应用系统。

5.1.4 网络日志分析流程

1. 日志的采集和存储

1）日志数据的采集

（1）标准协议接收：日志分析产品应能接收从日志数据源发送的基于 syslog、snmp trap、ftp 或其他标准协议的日志数据。

（2）代理方式采集：日志分析产品应能通过日志代理方式采集日志数据源的日志数据。

（3）日志文件导入：日志分析产品应能导入通用格式的日志文件。

2）日志数据的预处理

（1）数据筛选：日志分析产品应能基于既定策略对采集的日志数据进行过滤，有选择地生成日志记录。

（2）数据转换：日志分析产品应能将各种不同格式的原始日志数据转换为统一的数据格式，且转换时不能造成关键数据项丢失。

3）日志记录的生成

日志分析产品应在对采集的日志数据进行预处理和事件分析之后，生成相应的日志记录。日志记录内容应为管理员可理解，并且包含以下信息。

（1）事件发生的日期和时间；

（2）事件主体；

（3）事件客体；

（4）事件描述；

（5）事件类型；

（6）事件级别；

（7）日志数据源的 IP 地址或名称。

4）日志数据的存储

（1）安全保护：日志分析产品应采取安全机制，保护日志记录免遭未经授权的读取、删除或修改。

（2）防止日志记录丢失：日志分析产品应提供以下措施防止日志记录丢失。

① 日志记录应存储于非易失性存储介质中；

② 当日志记录的存储容量达到阈值时，发出报警信息；

③ 在日志记录的存储空间耗尽前，采用自动转储的方式将日志记录自动备份到其他的存储空间。

2. 日志的分析和处理

1）日志记录的处理

（1）数据整合

日志分析产品应能检查日志记录是否重复或无效，并进行数据的整合，即采用一定的技术手段对日志记录进行去重和有效性检查，以保证数据的有效性、一致性，以及减少冗余信息。

（2）数据拆分

若日志记录的单一字段包含多种信息并且这多种信息间具有分隔符，日志分析产品应能将此单一字段拆分成便于分析的若干字段存储。

2）日志记录的分析

（1）事件辨别

日志分析产品应能动态地维护一个事件库，对网络中的各种事件根据一定的特征进行分类，并且应能对采集的日志数据进行分析，判断日志数据所属的事件类型。

（2）事件定级

日志分析产品应为不同类型的事件设定其级别，以表明事件的性质或揭示此类事件的发生给信息系统所带来的危险程度。

（3）事件统计

日志分析产品应能够根据事件的以下属性进行统计。

① 事件主体；

② 事件客体；

③ 事件类型；

④ 事件级别；

⑤ 事件发生的日期和时间；

⑥ 日志数据源的 IP 地址或名称；

⑦ 事件的其他属性或属性的组合。

（4）潜在危害分析

日志分析产品应能设定单类事件累计发生次数或发生频率的阈值，当统计分析表明此类事件超出阈值时则表明信息系统出现了潜在的危害。

（5）异常行为分析

日志分析产品应维护一个与信息系统相关的合法用户的正常行为集合，以此区分入侵者的行为和合法用户的异常行为。