OSSEC Documentation

Release 2.7.2b1

Jeremy Rossi

January 29, 2014

Contents

OSPatrol is an Open Source Host-based Intrusion Detection System. It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, Mac OS X, Solaris and Windows. A list with all supported platforms is available at: *Supported Systems*

CHAPTER 1

Manual & FAQ

1.1 Manual

1.1.1 Getting started with OSPatrol

OSPatrol is a full platform to monitor and control your systems. It mixes together all the aspects of HIDS (host-based intrusion detection), log monitoring and SIM/SIEM together in a simple, powerful and open source solution. It is also backed and fully supported by Trend Micro.

Key Benefits

Compliance Requirements

OSPatrol helps customers meet specific compliance requirements such as PCI, HIPAA etc. It lets customers detect and alert on unauthorized file system modifications and malicious behavior embedded in the log files of COTS products as well as custom applications. For PCI, it covers the sections of file integrity monitoring (PCI 11.5, 10.5), log inspection and monitoring (section 10) and policy enforcement/checking.

Multi platform

OSPatrol lets customers implement a comprehensive host based intrusion detection system with fine grained application/server specific policies across multiple platforms such as Linux, Solaris, AIX, BSD, Windows, Mac OS X and VMware ESX.

Real-time and Configurable Alerts

OSPatrol lets customers configure incidents they want to be alerted on which lets them focus on raising the priority of critical incidents over the regular noise on any system. Integration with smtp, sms and syslog allows customers to be on top of alerts by sending these on to e-mail and handheld devices such as cell phones and pagers. Active response options to block an attack immediately is also available.

Integration with current infrastructure

OSPatrol will integrate with current investments from customers such as SIM/SEM (Security Incident Management/Security Events Management) products for centralized reporting and correlation of events.

Centralized management

OSPatrol provides a simplified centralized management server to manage policies across multiple operating systems. Additionally, it also lets customers define server specific overrides for finer grained policies.

Agent and agentless monitoring

OSPatrol offers the flexibility of agent based and agentless monitoring of systems and networking components such as routers and firewalls. It lets customers who have restrictions on software being installed on systems (such as FDA approved systems or appliances) meet security and compliance needs.

Key Features

File Integrity checking

There is one thing in common to any attack to your networks and computers: they change your systems in some way. The goal of file integrity checking (or FIM - file integrity monitoring) is to detect these changes and alert you when they happen. It can be an attack, or a misuse by an employee or even a typo by an admin, any file, directory or registry change will be alerted to you.

Covers PCI DSS sections 11.5 and 10.5.5.

Log Monitoring

Your operating system wants to speak to you, but do you know how to listen? Every operating system, application, and device on your network generate logs (events) to let you know what is happening. OSPatrol collects, analyzes and correlates these logs to let you know if something wrong is going on (attack, misuse, errors, etc). Do you want to know when an application is installed on your client box? Or when someone changes a rule in your firewall? By monitoring your logs, OSPatrol will let you know of that.

Covers PCI DSS section 10 in a whole.

Rootkit detection

Criminals (also known as hackers) want to hide their actions, but using rootkit detection you can be notified when they (or trojans, viruses, etc) change your system in this way.

Active response

Take immediate and automatic responses when something happens. Why wait for hours when you can alert your admin and block an attack right way?

1.1.2 OSPatrol Architecture

OSPatrol is composed of multiple pieces. It has a central manager monitoring everything and receiving information from agents, syslog, databases and from agentless devices.

Manager

The manager is the central piece of the OSPatrol deployment. It stores the file integrity checking databases, the logs, events and system auditing entries. All the rules, decoders and major configuration options are stored centrally in the manager, making it easy to administer even a large number of agents.

Agents

The agent is a small program or collection of programs installed on the systems you desire to monitor. The agent will collect information in real time and forward it to the manager for analysis and correlation. It has a very small memory and CPU footprint by default, not affecting system?x80x99s usage.

Agent security: It runs with a low privilege user (created during the installation) and inside a chroot jail isolated from the system. Most of the agent configuration is pushed from the manager, with just some of configuration stored locally on each agent. In case these local options are changed, the manager will receive the information and will generate an alert.

Agentless

For systems that you can't install an agent, OSPatrol allows you to perform file integrity monitoring on them without the agent installed. It can be very useful to monitor firewalls, routers and even Unix systems where you are not allowed to install the agent.

Virtualization/VMware

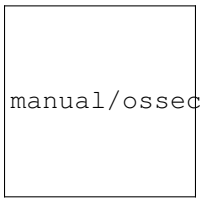
OSPatrol allows you to install the agent on the guest operating systems or inside the host (VMware ESX). With the agent installed inside VMware ESX you can get alerts about when a VM guest is being installed, removed, started, etc. It also monitors logins, logouts and errors inside the ESX server. In addition to that, OSPatrol performs the Center for Internet Security (CIS) checks for VMware, alerting if there is any insecure configuration option enabled or any other issue.

Firewalls, switches and routers

OSPatrol can receive and analyze syslog events from a large variety of firewalls, switches and routers. It supports all Cisco routers, Cisco PIX, Cisco FWSM, Cisco ASA, Juniper Routers, Netscreen firewall, Checkpoint and many others.

Architecture

This diagram shows the central manager receiving events from the agents and system logs from remote devices. When something is detected, active responses can be executed and the admin is notified.



Internal Architecture

For technical and deep detailed information on how it works, please read the following documents:

OSSEC log analysis/inspection architecture (PDF) - by Daniel Cid

This was the Architecture slide for OSSEC from which OSPatrol was forked from.

Support

1.1.3 Supported Systems

OSPatrol supports the following operating systems and log formats.

Operating Systems

The following operating systems are supported by the OSPatrol agent:

- GNU/Linux (all distributions, including RHEL, Ubuntu, Slackware, Debian, etc)
- Windows XP, 2003, Vista, 2008
- VMWare ESX 3.0,3.5 (including CIS checks)
- FreeBSD (all current versions)
- OpenBSD (all current versions)
- NetBSD (all current versions)
- Solaris 2.7, 2.8, 2.9 and 10
- AIX 5.2 and 5.3
- Mac OS X 10.x
- HP-UX 11

Devices supported via Syslog

These systems/devices are also supported via remote syslog:

- Cisco PIX, ASA and FWSM (all versions)
- Cisco IOS routers (all versions)
- Juniper Netscreen (all versions)
- SonicWall firewall (all versions)
- Checkpoint firewall (all versions)
- Cisco IOS IDS/IPS module (all versions)
- Sourcefire (Snort) IDS/IPS (all versions)
- Dragon NIDS (all versions)
- Checkpoint Smart Defense (all versions)
- McAfee VirusScan Enterprise (v8 and v8.5)
- Bluecoat proxy (all versions)

- Cisco VPN concentrators (all versions)
- VMWare ESXi 4.x

Devices and Operating Systems via Agentless

Using OSPatrol agentless options, the following systems are also supported (for log analysis and file integrity checking):

- Cisco PIX, ASA and FWSM (all versions)
- Cisco IOS routers (all versions)
- Juniper Netscreen (all versions)
- SonicWall firewall (all versions)
- Checkpoint firewall (all versions)
- All operating systems specified in the "operating systems" section

1.1.4 Installation

The best installation tutorial is available in the OSPatrol book.

OSPatrol HIDS Manager/Agent Installation

Installation of the OSPatrol HIDS is very simple. Just follow these few steps to have it working. Please make sure that you understand the type of installation you are choosing (manager, agent, local, or hybrid) and are also aware of the order (always install the manager first). If you don't know what I'm talking about, it's a good idea to visit the *install types page*.

Warning: Remember that when following this installation the commands only start after the # Everything before that is just the information about the prompt

Note: If you have experience with Unix, just download the latest version, uncompress it and run the "./install.sh" script.

1. Download the latest version and verify its checksum.

   Note: On some systems, the command md5, sha1 or wget may not exist, so try md5sum, sha1sum or lynx respectively instead.

```
# wget http://www.ospatrol.net/files/ospatrol-hids-2.6.tar.gz
# wget http://www.ospatrol.net/files/ospatrol-hids-2.6_checksum.txt
# cat ospatrol-hids-2.6_checksum.txt
MD5 (ospatrol-hids-2.6.tar.gz) = f4140ecf25724b8e6bdcaceaf735138a
SHA1 (ospatrol-hids-2.6.tar.gz) = 258b9a24936e6b61e0478b638e8a3bfd3882d91e
MD5 (ospatrol-agent-win32-2.6.exe) = 7d2392459aeab7490f28a10bba07d8b5
SHA1 (ospatrol-agent-win32-2.6.exe) = fdb5225ac0ef631d10e5110c1c1a8aa473e62ab4
# md5sum ospatrol-hids-2.6.tar.gz
MD5 (ospatrol-hids-2.6.tar.gz) = f4140ecf25724b8e6bdcaceaf735138a
# sha1sum ospatrol-hids-2.6.tar.gz
SHA1 (ospatrol-hids-2.6.tar.gz) = 258b9a24936e6b61e0478b638e8a3bfd3882d91e
```

2. Extract the compressed package and run the "./install.sh" script (It will guide you through the installation).

```
# tar -zxvf ospatrol-hids-*.tar.gz (or gunzip -d; tar -xvf)
# cd ospatrol-hids-*
# ./install.sh
```

3. Remember to open port 1514 (UDP) if there is a firewall between the server and the agents (not applicable to the local installation type).
4. If you are installing the server or the agent, remember to follow the *Managing the agents section*.
5. Start OSPatrol HIDS

```
# /var/ospatrol/bin/ospatrol-control start
```

OSPatrol HIDS agentless Installation

Agentless installation has its own page at: *Agentless Monitoring*.

OSPatrol HIDS Binary installation

On systems that do not have a C compiler or one is not allowed by policy installation can be done using *manual-install-binary*

OSPatrol Updates

Updating OSPatrol is as easy as it can get. Just download the latest package and follow the installation instructions as usual. It will detect that you already have it installed and ask:

```
- You already have OSPatrol installed. Do you want to update it? (y/n): y
- Do you want to update the rules? (y/n): y
```

Just say "yes" to these questions and it will update everything properly. Your local rules and configuration options will not be modified. The same applies to the Unix or Windows agent updates.

External installation documents

1.1.5 Agents

There are two types of agents within OSPatrol: installable agents and agentless agents. Installable agents are installed on hosts, and they report back to a central OSPatrol server via the OSPatrol encrypted message protocol. Agentless agents require no installation on remote hosts. They are processes initiated from the OSPatrol manager, which gather information from remote systems, and use any RPC method (e.g. ssh, snmp rdp, wmi).

Agent

Managing Agents

To add an agent to an OSPatrol manager with *manage_agents* you need to follow the steps below.

1. Run manage_agents on the OSPatrol server.
2. Add an agent.
3. Extract the key for the agent.

4. Copy that key to the agent.
5. Run manage_agents on the agent.
6. Import the key copied from the manager.
7. Restart the manager's OSPatrol processes.
8. Start the agent.

manage_agents on the OSPatrol server

The server version of manage_agents provides an interface to:

- add an OSPatrol agent to the OSPatrol server
- extract the key for an agent already added to the OSPatrol server
- remove an agent from the OSPatrol server
- list all agents already added to the OSPatrol server.

Running manage_agents and start screen `manage_agents` should be run as a user with the appropriate privileges (e.g. root).

Run `manage_agents`:

```
# /var/ospatrol/bin/manage_agents
```

The manage_agents menu:

```
****************************************
* OSPatrol HIDS v2.5-SNP-100809 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

Typing the appropriate letter and hitting enter will initiate that function.

Adding an agent To add an agent type `a` in the start screen:

```
Choose your action: A,E,L,R or Q: a
```

You are then prompted to provide a name for the new agent. This can be the hostname or another string to identify the system. In this example the agent name will be agent1.

```
- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: agent1
```

After that you have to specify the IP address for the agent. This can either be a single IP address (e.g. 192.168.1.25), a range of IPs (e.g. 192.168.2.0/24), or `any`. Using a network range or `any` is preferable when the IP of the agent may change frequently (DHCP), or multiple systems will appear to come from the same IP address (NAT).

```
* The IP Address of the new agent: 192.168.2.0/24
```

Warning: If you use a specific IP address it **must** be unique. Duplicate IP addresses will cause issues. Multiple systems can use the same IP range or `any`.

The last information you will be asked for is the ID you want to assign to the agent. *manage_agents* will suggest a value for the ID. This value should be the lowest positive number that is not already assigned to another agent. The ID 000 is assigned to the OSPatrol server. To accept the suggestion, simply press ENTER. To choose another value, type it in and press ENTER.

```
* An ID for the new agent[001]:
```

As the final step in creating an agent, you have to confirm adding the agent:

After that *manage_agents* appends the agent information to /var/ospatrol/etc/client.keys and goes back to the start screen.

Warning: If this is the first agent added to this server, the server's OSPatrol processes should be restarted using `/var/ospatrol/bin/ospatrol-control restart`.

Extracting the key for an agent

After adding an agent, a key is created. This key must be copied to the agent. To extract the key, use the `e` option in the manage_agents start screen. You will be given a list of all agents on the server. To extract the key for an agent, simply type in the agent ID. It is important to note that you have to enter all digits of the ID.

```
Choose your action: A,E,L,R or Q: e

Available agents:
   ID: 001, Name: agent1, IP: 192.168.2.0/24
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
MDAyIGFnZW50MSAxOTIuMTY4LjIuMC8yNCBlNmY3N2RiMTdmMTJjZGRmZjg5YzA4ZDk5m

** Press ENTER to return to the main menu.
```

The key is encoded in the string (shortened for this example) `MDAyIGFnZW50MSAxOTIuMTY4LjIuMC8yNCBlNmY3N2RiMTdmMTJ` and includes information about the agent. This string can be added to the agent through the agent version of `manage_agents`.

Removing an agent

If you want to remove an OSPatrol agent from the server, use the `r` option in the *manage_agents* start screen. You will be given a list of all agents already added to the server. To remove an agent, simply type in the ID of the agent, press enter, and finally confirm the deletion. It is important to note that you have to enter all digits of the ID.

```
Choose your action: A,E,L,R or Q: e

Available agents:
   ID: 001, Name: agent1, IP: 192.168.2.0/24
Provide the ID of the agent to extract the key (or '\q' to quit): 001
Confirm deleting it?(y/n): y
Agent '001' removed.
```

`manage_agents` then invalidates the agent information in `/var/ospatrol/etc/client.keys`. Only the values for ID and the key are kept to avoid conflicts when adding agents. The deleted agent can no longer communicate with the OSPatrol server.

manage_agents on OSPatrol agents

The agent version provides an interface for importing authentication keys.

```
**************************************
* OSPatrol HIDS v2.5-SNP-100809 Agent manager.     *
* The following options are available: *
**************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: i

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): [key extracted via manage_agents on the server]

Agent information:
   ID:001
   Name:agent1
   IP Address:192.168.2.0/24

Confirm adding it?(y/n): y
Added.
** Press ENTER to return to the main menu.
```

For the changes to be in effect you have to restart the server and start the agent.

Agent systems behind NAT or with dynamic IPs (DHCP)

If you want to install the agent on systems without a static IP address or behind a NAT device, you need to configure the agent using a CIDR address or the ip address of `any`.

DHCP Example

To add an agent that can receive any IP address in the 192.168.2.0/24 network, just provide the IP address of the agent as 192.168.2.0/24. Example (taken from manage_agents):

```
Please provide the following:
* A name for the new agent: test
* The IP Address of the new agent: 192.168.2.0/24
```

NAT Example

The same applies to systems behind a NAT device. The OSPatrol server will see all agents behind the NAT as if they have the same IP address.

For example, you have systems 192.168.1.2, 192.168.1.3 and 192.168.1.4 behind a nat server that connects to network 10.1.1.0/24 with the ospatrol server on it.

In this case, you need to config the agents as if their IP was 10.1.1.0/24, because this is the IP that the server is seeing (not their original IP). Using `any` instead of an IP address or range is also a valid option, allowing the agent to connect from any IP address.

On the *manage_agents* tool, add each one of those agents on the server using the following format:

```
Please provide the following:
* A name for the new agent: agent-1
* The IP Address of the new agent: 10.1.1.0/24

Please provide the following:
* A name for the new agent: agent-2
* The IP Address of the new agent: any
```

Note: Make sure to use one separate key for each agent.

Centralized agent configuration

If you ever wanted to be able to configure your agents remotely, you will be happy to know that starting on version 2.1 you will be able to do so. We allow centralized configuration for file integrity checking (syscheckd), rootkit detection (rootcheck) and log analysis.

This is how it works.

Create agent configuration

First Create the file /var/ospatrol/etc/shared/agent.conf.

Inside the file you can configure the agent just as you would normally at ospatrol.conf

```
<agent_config>
    <localfile>
        <location>/var/log/my.log</location>
        <log_format>syslog</log_format>
    </localfile>
</agent_config>
```

But you have a few more options. You can restrict the config by agent name, operating system, or profile:

```
<agent_config name="agent1">
    <localfile>
        <location>/var/log/my.log</location>
        <log_format>syslog</log_format>
    </localfile>
</agent_config>

<agent_config os="Linux">
    <localfile>
        <location>/var/log/my.log2</location>
        <log_format>syslog</log_format>
    </localfile>
</agent_config>

<agent_config os="Windows">
    <localfile>
        <location>C:\myapp\my.log</location>
```

```
        <log_format>syslog</log_format>
    </localfile>
</agent_config>
```

And only the proper agent will read them, giving us great granularity to push the configuration to all your agents.

After you configured, the manager will push it to the agents. Note that it can take a while for it to complete (since the manager caches the shared files and only re-reads them every few hours). If you restart the manager the configuration will be pushed much quicker.

Restart the agent

Once the configuration file is pushed, you can run the command *agent_control* to see if the agent received the config and restart the agent remotely.

```
# md5sum /var/ospatrol/etc/shared/agent.conf
MD5 (/var/ospatrol/etc/shared/agent.conf) = ee1882236893df851bd9e4842007e7e7
# /var/ospatrol/bin/agent_control -i 200

OSPatrol HIDS agent_control. Agent information:
Agent ID: 200
Agent Name: ourhome
IP address: 192.168.0.0/16
Status: Active

Operating system: Linux ourhome 2.6.24-23-generic #1 SMP Mon Jan 26 00..
Client version: OSPatrol HIDS v2.1 / ee1882236893df851bd9e4842007e7e7
Last keep alive: Tue Jun 30 08:29:17 2009

Syscheck last started at: Tue Jun 30 04:29:32 2009
Rootcheck last started at: Tue Jun 30 06:03:08 2009
```

When the agent received the configuration, the "Client Version" field will have the md5sum of the agent.conf file.

Note: Linux systems generally use `md5sum`, but other systems may use `md5` as the name of the application to check the hash of the file.

To restart the agent:

```
# /var/ospatrol/bin/agent_control -R 200 (where 200 is the agent id)

OSPatrol HIDS agent_control: Restarting agent: 200
```

Agentless

Agentless Monitoring

Agentless monitoring allows you to run integrity checking on systems without an agent installed (including routers, firewalls, switches and even Linux/BSD systems). It can be executed just like our normal file integrity checking (alerting of checksum changes) or doing diffs and showing exactly what has changed.

Agentless configuration options

`agentless`
: This is the section that will contain the agentless configuration.

frequency
This controls the number of seconds between each run.

host
This defines the username and agentless host.

Example:

```
<host>root@linux.server.example.com</host>
```

state
This determines whether the checks are periodic or periodic_diff.

- periodic: The output from the scripts is processed by the OSPatrol processes.
- periodic_diff: The output from the scripts is compared to the output of previous runs.

arguments
This defines the arguments passed to the script.

Check *_manual-agentless-scripts* for more information.

Getting started with agentless

After you installed OSPatrol, you need to enable the agentless monitoring:

```
# /var/ospatrol/bin/ospatrol-control enable agentless
```

And provide the SSH authentication to the host you want to access. For Cisco devices (PIX, routers, etc), you need to provide an additional parameter for the enable password. The same thing applies if you want to add support for "su", it must be the additional parameter. In this example, I am adding a Linux box (example.net) and a PIX firewall (pix.fw.local):

```
# /var/ospatrol/agentless/register_host.sh add root@example.net mypass1
  *Host root@example.netl added.
# /var/ospatrol/agentless/register_host.sh add pix@pix.fw.local pixpass enablepass
  *Host pix@pix.fw.local added.

# /var/ospatrol/agentless/register_host.sh list
  *Available hosts:
pix@pix.fw.local
root@example.net
```

If you want to use public key authentication instead of passwords, you need to provide NOPASS as the password and create the public key:

```
# sudo -u ospatrol ssh-keygen
```

It will create the public keys inside /var/ospatrol/.ssh . After that, just scp the public key to the remote box and your password less connection should work.

Configuring agentless

Once you have added all your systems, you need to configure OSPatrol to monitor them. By default, we have 4 agentless types (but we plan to add more soon):

- ssh_integrity_check_bsd
- ssh_integrity_check_linux

- ssh_generic_diff
- ssh_pixconfig_diff

For the first two, you give a list of directories in the configuration and OSPatrol will do the integrity checking of them on the remote box. On the ssh_generic_diff, you give a set of commands to run on the remote box and OSPatrol will alert when the output of them changes. The ssh_pixconfig_diff will alert when a Cisco PIX/router configuration changes.

So, for my first system (root@example.net), I will monitor the /bin, /etc and /sbin directories every 10 hours (if I was using the ssh_integrity_check_bsd, the argument would be the directories as well):

```
<agentless>
    <type>ssh_integrity_check_linux</type>
    <frequency>36000</frequency>
    <host>root@example.net</host>
    <state>periodic</state>
    <arguments>/bin /etc/ /sbin</arguments>
</agentless>
```

For my PIX, the configuration looks like:

```
<agentless>
    <type>ssh_pixconfig_diff</type>
    <frequency>36000</frequency>
    <host>pix@pix.fw.local</host>
    <state>periodic_diff</state>
</agentless>
```

And just to exemplify the ssh_generic_diff I will also monitor ls -la /etc; cat /etc/passwd on the root@example.net. Note that if you want to monitor any network firewall or switch, you can use the ssh_generic_diff and just specify the commands in the arguments option. To use "su", you need to set the value "use_su" before the hostname (eg: <host>use_su root@example.net</host>).

```
<agentless>
    <type>ssh_generic_diff</type>
    <frequency>36000</frequency>
    <host>root@example.net</host>
    <state>periodic_diff</state>
    <arguments>ls -la /etc; cat /etc/passwd</arguments>
</agentless>
```

Running the completed setup

Once the configuration is completed, you can restart OSPatrol. You should see something like "Started ospatrol-agentlessd" in the output. Before each agentless connection is started, OSPatrol will do a configuration check to make sure everything is fine. Look at /var/ospatrol/logs/ospatrol.log for any error. If you see:

It means that you don't have the expect library installed on the server (it is not necessary to install anything on the agentless systems to monitor). On Ubuntu you can do the following to install:

```
# apt-get install expect
```

After installing expect, you can restart OSPatrol and you should see:

When it connects to the remote system, you will also see:

Alerts

These are some of the alerts you will get:

For the ssh_generic_diff:

```
OSPatrol HIDS Notification.
2008 Dec 12 01:58:30

Received From: (ssh_generic_diff) root@example.net->agentless
Rule: 555 fired (level 7) -> "Integrity checksum for agentless device changed."
Portion of the log(s):

ospatrol: agentless: Change detected:
35c35
< -rw-r-r- 1 root wheel 34 Dec 10 03:55 hosts.deny
--
> -rw-r-r- 1 root wheel 34 Dec 11 18:23 hosts.deny
-END OF NOTIFICATION
```

For the PIX:

```
OSPatrol HIDS Notification.
2008 Dec 01 15:48:03

Received From: (ssh_pixconfig_diff) pix@pix.fw.local->agentless
Rule: 555 fired (level 7) -> "Integrity checksum for agentless device changed."
Portion of the log(s):

ospatrol: agentless: Change detected:
48c48
< fixup protocol ftp 21
--
> no fixup protocol ftp 21
100c100
< ssh timeout 30
--
> ssh timeout 50
More changes..

-END OF NOTIFICATION
```

Contents

Writing Agentless Scripts

All scripts that work with OSPatrol agentless security monitoring use stdout for communication and reporting to the OSPatrol server. This makes writing scripts for OSPatrol simple as you do not need to do anything more then print or

echo to stdout. The format of the output does need to meet the OSPatrol specification, but that is a very simple thing to do.

Agentless Script Types

Before we move to the specification details I need to explain that OSPatrol agentless runs to different types of scripts. Namely the following:

- **periodic_diff**
  - Scripts output data to the OSPatrol agentless process that will then be compared to past runs and if there are differences an OSPatrol alert will be generated.
- **periodic**
  - Scripts output controlled messages to the OSPatrol agentless process that will then be processed accordingly.

Periodic diff Specification The output for periodic_diff is very simple, any and all output after the agentless command `STORE: now` and before the next OSPatrol Command will be stored and compared for differences. This type of script is mostly used for hardware devices such as Cisco IOS, Juniper JunOS, and other products.

Scripts that use the periodic_diff make use of the following commands:

- **INFO:**
  - The string following INFO will be logged to /var/ospatrol/logs/ospatrol.log by OSPatrol for debugging.
- **ERROR:**
  - Error needs to be reported. The string following this command is forwarded to the OSPatrol manager, and the OSPatrol process closes down the script.
- **STORE:**
  - All the lines that follows this command will be added stored and compared to previous runs of the script

Here is an example of a periodic_diff script that comes with OSPatrol. (Please note with all agentless scripts you must be in the root of the OSPatrol install for them to function correctly.)

```
obsd46#( cd /var/ospatrol && ./agentless/ssh_pixconfig_diff cisco@172.17.0.1 'show hardware' )
spawn ssh -c des cisco@172.17.0.1
No valid ciphers for protocol version 2 given, using defaults.
Password:

a.zfw.tss>INFO: Starting.
enable
Password:
a.zfw.tss#ok on enable pass

STORE: now
no pager
          ^
% Invalid input detected at '^' marker.

a.zfw.tss#term len 0
a.zfw.tss#terminal pager 0
                   ^
% Invalid input detected at '^' marker.
```

```
a.zfw.tss#show version | grep -v Configuration last| up
                         ^
% Invalid input detected at '^' marker.

a.zfw.tss#show running-config
Building configuration...


Current configuration : 14631 bytes
!
version 12.4

[................SNIP CONFIG.................]

a.zfw.tss#show hardware
Cisco IOS Software, 3800 Software (C3845-ADVENTERPRISEK9-M), Version 12.4(24)T1, RELEASE SOFTWARE (fc
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Fri 19-Jun-09 19:21 by prod_rel_team

ROM: System Bootstrap, Version 12.3(11r)T2, RELEASE SOFTWARE (fc1)

a.zfw.tss uptime is 1 week, 5 days, 7 hours, 29 minutes
System returned to ROM by reload at 13:34:26 UTC Thu Oct 22 2009
System image file is "flash:c3845-adventerprisek9-mz.124-24.T1.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 3845 (revision 1.0) with 1007615K/40960K bytes of memory.
Processor board ID FTX1043A2CR
2 Gigabit Ethernet interfaces
1 ATM interface
1 Virtual Private Network (VPN) Module
4 CEM T1/E1 ports
DRAM configuration is 64 bits wide with parity enabled.
479K bytes of NVRAM.
492015K bytes of USB Flash usbflash0 (Read/Write)
62720K bytes of ATA System CompactFlash (Read/Write)

Configuration register is 0x2102


a.zfw.tss#exit
Connection to 172.17.0.1 closed by remote host.
```

```
Connection to 172.17.0.1 closed.

INFO: Finished.
```

In this example above the script would store the contents between `STORE: now` and `INFO: Finished.`. If this is the first time that OSPatrol agentless has run this command no alerts would be generated and the contents would have been saved for later comparisons. If OSPatrol agentless has a stored copy from a previous execution it will compare the files and if there are any differences it will generate an alert.

Periodic Specification The periodic specification has more options and gives more control to the script writer on what actions OSPatrol will take. Once again stdout is used for communication so script writing is easy.

- **INFO:**
  - The string following INFO will be logged to /var/ospatrol/logs/ospatrol.log by OSPatrol for debugging.
- **ERROR:**
  - Error needs to be reported. The string following this command is forwarded to the OSPatrol manager, and the OSPatrol process closes down the script.
- **FWD:**
  - The string following FWD is a colon delimited list of stats on a given file.
- **LOG:**
  - The string following LOG: will be passed into ospatrol-analysisd and processed like all other log messages.

Example of real FWD: command.

```
FWD: 19419:600:0:0:fb30de5b02029950ae05885a3d407c8c:017cd6118cdc166ee8eba8af1b7fdad6763203d3 ./.bash_
```

The Fields break down in to the following:

- FWD:
  - The OSPatrol Command
- 19419
  - Total size of file, in bytes
- 600
  - Access rights of file in octal
- 0
  - User ID of file owner
- 0
  - Group ID of file owner
- fb30de5b02029950ae05885a3d407c8c
  - MD5 Hash of file
- 017cd6118cdc166ee8eba8af1b7fdad6763203d3
  - SHA1 Hash of file
- ./.bash_history
  - Path and name of file

Using this format OSPatrol can store the information about a file and then in the future run compare that they are the same. If for some reason they are not the same an alert will be generated. Here is an example of a password change on a linux system:

```
OSPatrol HIDS Notification.
2009 Sep 21 15:19:00

Received From: (ssh_integrity_check_linux) root@172.17.20.20->syscheck
Rule: 550 fired (level 7) -> "Integrity checksum changed."
Portion of the log(s):

Integrity checksum changed for: '/etc/shadow'
Old md5sum was: '0d92e12c92f3edcf9d8876ea57c5f677'
New md5sum is : '2bd51b61dea17c5682fb2c0cf4f92c63'
Old sha1sum was: '2270c03a920ef8dd50e11cefdef046a8660f7a29'
New sha1sum is : 'd9518ea9022b10d07f81925c6d7f2abb4364b548'

--END OF NOTIFICATION
```

Agentless Script: ssh_integrity_check_linux

Now that we have an understanding of how agentless scripts communicate with the parent OSPatrol process, let's move on to a working example. The OSPatrol supplied script `ssh_integrity_check_linux` is a great place to start, so lets open it up and see what is going on.

```
obsd46# cat /var/ospatrol/agentless/ssh_integrity_check_linux
 #!/usr/bin/env expect

 # @(#) $Id: ssh_integrity_check_linux,v 1.11 2009/06/24 17:06:21 dcid Exp $
 # Agentless monitoring
 #
 # Copyright (C) 2009 Trend Micro Inc.
 # All rights reserved.
 #
 # This program is a free software; you can redistribute it
 # and/or modify it under the terms of the GNU General Public
 # License (version 3) as published by the FSF - Free Software
 # Foundation.


 # Main script.
source "agentless/main.exp"


 # SSHing to the box and passing the directories to check.
if [catch {
    spawn ssh $hostname
} loc_error] {
    send_user "ERROR: Opening connection: $loc_error.\n"
    exit 1;
}


source $sshsrc
source $susrc

set timeout 600
```

```
send "echo \"INFO: Starting.\"; for i in `find $args 2>/dev/null`;do tail \$i >/dev/null 2>&1 &&
md5=`md5sum \$i | cut -d \" \" -f 1` && sha1=`sha1sum \$i | cut -d \" \" -f
 1` && echo FWD: `stat --printf \"%s:%a:%u:%g\" \$i`:\$md5:\$sha1 \$i; done; exit\r"
send "exit\r"

expect {
    timeout {
        send_user "ERROR: Timeout while running commands on host: $hostname .\n"
        exit 1;
    }
    eof {
        send_user "\nINFO: Finished.\n"
        exit 0;
    }
}

exit 0;
```

The comments in the script hints to what is going on, but everything up to and including set timeout 600 is related to setting up the expect functions and code for handling the ssh subprocess and connecting to the remote host. I am not going to spend any time with this section, I am just going to make use of it.

The meat of what is getting processed on the remote end all happens in two lines.

```
send "echo \"INFO: Starting.\"; for i in `find $args 2>/dev/null`;do tail \$i >/dev/null 2>&1 &&
md5=`md5sum \$i | cut -d \" \" -f 1` && sha1=`sha1sum \$i | cut -d \" \" -f
 1` && echo FWD: `stat --printf \"%s:%a:%u:%g\" \$i`:\$md5:\$sha1 \$i; done; exit\r"
```

Let's break this down to see what is happening.

The send command pushes the following string to the ssh subprocess which gets run on the remote end of the connection. Before the script is sent to the remote host expect internally processes the string. This includes searching for variables and removing any control characters.

The control characters are first taken into account, and in the case of our example all escaped special characters are processed. ", r, and $ would be replaced with ", "carriage return", and & respectively. The reason the escape characters are needed so that they will not interfere with expects own string processing and control. We will need to handle control characters in this way when we begin writing our own script.

While special characters were being handled by expect it also looked for variables to replace, in this case it will find $args and replace it with what ever arguments were passed to the script by the OSPatrol agentless process. If we specified the following in `/var/ospatrol/etc/ospatrol.conf` the $args variable would be replaced with `/bin /etc /sbin`.

```
<agentless>
    <type>ssh_integrity_check_linux</type>
    <frequency>3600</frequency>
    <host>root@172.17.20.20</host>
    <state>periodic</state>
    <arguments>/bin /etc /sbin</arguments>
</agentless>
```

Back to the commands that get run. Once expect has completed replacement we are left with this command.

```
echo "INFO: Starting."; for i in `find /bin /etc /sbin 2>/dev/null`;do tail $i >/dev/null 2>&1 &&
md5=`md5sum $i | cut -d " " -f 1` && sha1=`sha1sum $i | cut -d " " -f
 1` && echo FWD: `stat --printf "%s:%a:%u:%g" $i`:$md5:$sha1 $i; done; exit
    exit
```

This script then goes and uses the Unix find command to locate all files in the specified path (from the arguments

passed) and generates an OSPatrol FWD: command for each one and prints it to stdout. Making use of the commands stat, md5sum, and sha1sum to generate the data needed. Here is an example of the output checking.

```
spawn ssh root@172.17.20.20
Last login: Wed Nov  4 11:32:51 2009 from 172.17.20.131^M
[linux26 ~]#
INFO: Started.
echo "INFO: Starting."; for i in `find {/bin /etc /sbin} 2>/dev/null`;do tail $i >/dev/null 2>&1 &&
md5=`md5sum $i | cut -d " " -f 1` && sha1=`sh a1sum $i | cut -d " " -f
 1` && echo FWD: `stat --printf "%s:%a:%u:%g" $i`:$md5:$sha1 $i; done; exit
INFO: Starting.
FWD: 833:644:0:0:4148adea745af5121963f6b731b60013:60877a6f6981b16c0d53d32bcd3f07d41cfb5bd4 /etc/modpr
glib2.sh
[...........SNIP...........]
FWD: 1696:644:0:0:c2bd306b205ad9e81fb02ce6b225d384:5244d65815cb228a4fac7bc4c1c7774508fb7505 /etc/nssw
FWD: 85179:644:0:0:8db574225cd1068b47e77ceccd96f8ff:b5ef6183b35ee9d1b66ed2cefe98003c5bd99192 /etc/ser
FWD: 49:644:0:0:52c3df2f1edf30ca3db82174be3a68d2:1934648f2429b70b1f729d343a6956fb0ea73136 /etc/php.d/
FWD: 873:644:0:0:04559d1fe27ecd079b69df8b319f937e:e5cab1bf1f9e4bc4386309f4e00a9b7be3e543a2 /etc/php.c
FWD: 59:644:0:0:94636ba6c4bac9d8d49d9de1a513ae0c:41d5164a2c6e332e40edf55c59a2d0df8a260964 /etc/php.d/
FWD: 49:644:0:0:917dbbafbfaaa20f660063d627123dae:0e829d4ffc69f58dc258510b4b8452412e31ccc5 /etc/php.d/
FWD: 0:644:0:0:d41d8cd98f00b204e9800998ecf8427e:da39a3ee5e6b4b0d3255bfef95601890afd80709 /etc/wvdial
logout
Connection to 172.17.20.20 closed.

INFO: Finished.
```

Modifying to make own Agentless Script: ssh_dmz_linux

Using the built in OSPatrol agentless scripts are great, but sometimes we need more focused scanning and checking. So let's modify the ssh_integrity_check_linux for our environment.

The goals for this new script will be to watch for changes to files based on the following criteria:

- All setuid and setgid files
- All files related to authentication (including .htaccess and ssh files)
- All application specific files (apache, ssh)

Finding all setuid and setgid files

Let's first start by identifying a method to locate all files with their setuid or setgid bits enabled. To do this we will ssh to the host 172.17.20.20 and use find to locate the files.

```
obsd46# sudo -u ospatrol ssh root@172.17.20.20
[linux26 ~]# find / -type f \( -perm -4000 -o -perm -2000 \)
/sbin/umount.nfs
/sbin/netreport
/sbin/unix_chkpwd
/sbin/mount.nfs
/sbin/pam_timestamp_check
/sbin/mount.nfs4
/sbin/umount.nfs4
/bin/ping6
/bin/su
/bin/umount
/bin/ping
/bin/mount
/lib/dbus-1/dbus-daemon-launch-helper
```

```
/usr/libexec/openssh/ssh-keysign
/usr/libexec/utempter/utempter
/usr/sbin/usernetctl
/usr/sbin/postqueue
/usr/sbin/userhelper
/usr/sbin/userisdnctl
/usr/sbin/postdrop
/usr/sbin/suexec
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/locate
/usr/bin/wall
/usr/bin/sudoedit
/usr/bin/gpasswd
/usr/bin/lockfile
/usr/bin/newgrp
/usr/bin/write
/usr/bin/screen
/usr/bin/passwd
/usr/bin/chage
/usr/bin/sperl5.8.8
/usr/bin/crontab
/usr/bin/ssh-agent
```

Finding all files related to authentication and applications specific files

Finding all files with setuid and setgid was simple, but finding all files related to authentication is more involved. This of course will vary from system to system, but this should be good starting point.

```
obsd46# sudo -u ospatrol ssh root@172.17.20.20
[linux26 ~]# find / \( -name ".ssh" -o -name "ssh" -o -name "sshd" -o -name "httpd" -o -name ".htacce
-o -name "pam.d" \) -exec find {} \;
/var/www/html/admin/modules/framework/var/www/html/admin/modules/.htaccess
/etc/httpd
/etc/httpd/conf
/etc/httpd/conf.d
/etc/httpd/conf.d/php.conf
/etc/httpd/conf.d/proxy_ajp.conf
/etc/httpd/conf.d/README
/etc/httpd/conf.d/ssl.conf
/etc/httpd/conf.d/welcome.conf
/etc/httpd/conf/httpd.conf
/etc/httpd/conf/magic
/etc/httpd/logs
/etc/httpd/modules
/etc/httpd/run
/etc/logrotate.d/httpd
/etc/pam.d
/etc/pam.d/authconfig
[...................SNIP PAM Files.....................]
/etc/pam.d/system-config-network-cmd
/etc/pam.d/vsftpd
/etc/rc.d/init.d/httpd
/etc/rc.d/init.d/sshd
/etc/ssh
/etc/ssh/ssh_config
/etc/ssh/sshd_config
/etc/ssh/ssh_host_dsa_key
```

```
/etc/ssh/ssh_host_dsa_key.pub
/etc/ssh/ssh_host_key
/etc/ssh/ssh_host_key.pub
/etc/ssh/ssh_host_rsa_key
/etc/ssh/ssh_host_rsa_key.pub
/etc/sysconfig/httpd
/root/.ssh
/root/.ssh/authorized_keys
/usr/bin/ssh
/usr/lib/httpd
/usr/lib/httpd/modules
/usr/lib/httpd/modules/libphp5.so
[..................SNIP Apache modules.............]

/usr/lib/httpd/modules/mod_vhost_alias.so
/usr/sbin/httpd
/usr/sbin/sshd
/usr/src/tbm-pbxconfig-5.5.1/amp_conf/htdocs/admin/modules/framework/htdocs/admin/modules/.htaccess
/usr/src/tbm-pbxconfig-5.5.1/amp_conf/htdocs/admin/modules/.htaccess
/var/empty/sshd
/var/empty/sshd/etc
/var/empty/sshd/etc/localtime
/var/www/html/admin/modules/framework/var/www/html/admin/modules/.htaccess
/var/www/html/admin/modules/.htaccess
```

Merging finds

Now we have two basic find methods that identify the files we want to monitor for changes, but our finds were a little greedy so we should create a way to strip out unwanted files from the list. As this is a unix system egrep is the king for finding or removing items from a list. To simplify things we can use egrep with the -v command line argument which tells egrep NOT to print any matching items.

Just to make sure that we do not end up double processing files we can make use of the sort command with -u argument to remove any duplicates.

Here is how we would put together both finds, egrep, and sort to locate and filter what is needed.

```
( find / -type f \( -perm -4000 -o -perm -2000 \) && \find / \( -name ".ssh" -o -name "ssh" -o -name
-o -name "httpd" -o -name ".htaccess" -o -name "pam.d" \) -exec find {} \; ) 2>/dev/null | egrep
-v "known_hosts|moduli|var\/log|var\/lock" | sort -u
```

The above command we have found all files and paths that we would like to monitor, but this still needs to be integrated into a script on the OSPatrol server.

Creating ssh_dmz_linux

We don't want to make changes to ssh_integrity_check_linux directly so we will need to make a copy.

```
obsd46# (cd /var/ospatrol/agentless && cp ssh_integrity_check_linux ssh_dmz_linux)
```

Integrating our new command line into the script we must pay close attention to special characters that expect will process. Due to this we will need to escape all / and " by proceeding them with . Once we are done escaping we just insert our new line in place of find $args 2>/dev/null in our new file.

Here is what the completed script will look like.

```
obsd56# cat /var/ospatrol/agentless/ssh_dmz_linux
 #!/usr/bin/env expect

 # @(#) $Id: ssh_integrity_check_linux,v 1.11 2009/06/24 17:06:21 dcid Exp $
 # Agentless monitoring
```

```
 #
 # Copyright (C) 2009 Trend Micro Inc.
 # All rights reserved.
 #
 # This program is a free software; you can redistribute it
 # and/or modify it under the terms of the GNU General Public
 # License (version 3) as published by the FSF - Free Software
 # Foundation.


 # Main script.
source "agentless/main.exp"


 # SSHing to the box and passing the directories to check.
if [catch {
    spawn ssh $hostname
} loc_error] {
    send_user "ERROR: Opening connection: $loc_error.\n"
    exit 1;
}


source $sshsrc
source $susrc

set timeout 600
send "echo \"INFO: Starting.\"; for i in `(find / \\( -name \".ssh\" -o -name \"ssh\" -o -name \"ssho
-o -name \"httpd\" -o -name \".htaccess\" -o -name \"pam.d\" \\) -exec find {} \\; && find / -type f
\\( -perm -4000 -o -perm -2000 \\); ) 2>/dev/null | egrep -v \"known_hosts|moduli|var\\/log|var\\/loc
do tail \$i >/dev/null 2>&1 && md5=`md5sum \$i | cut -d \" \" -f 1` && sha1=`sha1sum \$i | cut -d \"
-f 1` && echo FWD: `stat --printf \"%s:%a:%u:%g\" \$i`:\$md5:\$sha1 \$i; done; exit\r"
send "exit\r"

expect {
    timeout {
        send_user "ERROR: Timeout while running commands on host: $hostname .\n"
        exit 1;
    }
    eof {
        send_user "\nINFO: Finished.\n"
        exit 0;
    }
}

exit 0;
```

Testing

Before we add this new script to OSPatrol configuration we need to test it.

```
obsd46# (cd /var/ospatrol && sudo -u ospatrol ./agentless/ssh_dmz_linux root@172.17.20.20 )

ERROR: ssh_integrity_check <hostname> <arguments>
```

Due to not making use of the of the $arg variable in the way that ssh_integrity_check_linux wants use too, this caused this the problem above. Solving this problem would require making changes to files that will effect other built in scripts. So a quick solution is to just pass anything as an argument to the script. This will have no effect on our script as we do not make use of the $arg variable.

```
obsd46# (cd /var/ospatrol && sudo -u ospatrol ./agentless/ssh_dmz_linux root@172.17.20.20 NOTUSED)
spawn ssh root@172.17.20.20
Last login: Wed Nov  4 13:46:32 2009 from 172.17.20.131^M
[linux26 ~]#
INFO: Started.
echo "INFO: Starting."; for i in `(find / \( -name ".ssh" -o -name "ssh" -o -name "sshd" -o -name "ht
-o -name ".htaccess" -o -name "pam.d" \)  -exec find {} \; && find / -type f \( -perm -4000 -o -perm
\); ) 2>/dev/null | egrep -v "known_hosts|moduli|var\/log|var\/lock"`;do tail $i >/dev/null 2>&1 &&
 md5=`md5s ^Mum $i | cut -d " " -f 1` && sha1=`sha1sum $i | cut -d " " -f 1` && echo FWD: `stat --pri
"%s:%a:%u:%g" $i`:$md5:$sha1 $i; done; exit
INFO: Starting.
FWD: 14:775:100:101:3bc0a3e92f8170084dd102eda9a474b1:25a1783a3c6bdd9745ec245ec1bfa0414ee05d23 /var/ww
FWD: 3519:644:0:0:e4ca381035a34b7a852184cc0dd89baa:6e43d0b5a46ed5ba78da5c7e9dcf319b27d769e7 /var/empt
FWD: 560:644:0:0:58370830ecfa056421ad21aff9c18905:d115bb5aeefaab97c53fbbd5df84ebcb9170d796 /etc/httpd
[...................SNIP.............................]
FWD: 392:644:0:0:e92bea7e9d70a9ecdc61edd7c0a2f59a:d77b61dac010c60589b4d8a2039e3b8a5bed18b2 /etc/httpd
FWD: 70888:4711:0:0:9046bd13339e7ef22266067b633e601a:3fc41029ddb14fe4ed613f479fa9e89c944f04dd /usr/bi
FWD: 315416:6755:0:0:4c63a9709fb7f0f97c30aa29d204859c:c379efa658de72866b8f6de5767906ff78d127b0 /usr/b
FWD: 88964:2755:0:99:baf3ebef6377d6ef42858776c33621b0:62394bf57d18c3fd49adeb39a1da61661cabc3c8 /usr/b
logout
Connection to 172.17.20.20 closed.

INFO: Finished.
```

1.1.6 Log monitoring/analysis

Log Analysis (or log inspection) is done inside OSPatrol by the logcollector and analysisd processes. The first one collects the events and the second one analyzes (decodes, filters and classifies) them.

It is done in real time, so as soon as an event is written OSPatrol will process them. OSPatrol can read events from internal log files, from the Windows event log and also receive them directly via remote syslog.

What is log analysis?

Inside OSPatrol we call log analysis a LIDS, or log-based intrusion detection. The goal is to detect attacks, misuse or system errors using the logs.

LIDS - Log-based intrusion detection or security log analysis are the processes or techniques used to detect attacks on a specific network, system or application using logs as the primary source of information. It is also very useful to detect software misuse, policy violations and other forms of inappropriate activities.

Quick Facts

- How often are logs monitored?
  - In real time.
- Where are the events analyzed?
  - In the manager.
- How long are they stored?
  - For as long as your policy dictates (it is user configurable).
- Where does this help me with compliance?

  - (PCI DSS, etc) It helps with the whole section 10 (log monitoring) of PCI.
- How much CPU does it use?
  - On the agent, it uses very little CPU/memory since it just read the events and forwards them to the manager.
  - On the manager, it depends on the number of events per second (EPS).
- How does it deal with false positives?
  - False positives can be eliminated using local rules.

Configuration Options

These options should be specified locally in each agent's ospatrol.conf file or the share agent.conf. Inside the `<localfile>` element, you can have the following options.

`localfile`

`location`
Specify the location of the log to be read. strftime formats may be used for log file names. For instance, a log file named `file.log-2011-01-22` could be referenced with `file.log-%Y-%m-%d`. Wildcards may be used on non-Windows systems. When wildcards are used, the log files must exist at the time `ospatrol-logcollector` is started. It will not automatically begin monitoring new log files. `strftime` and wildcards cannot be used on the same entry.

Default: Multiple (eg /var/log/messages)

Allowed: Any log file

`log_format`
The format of the log being read.

Note: If the log has one entry per line, use syslog.

Default: syslog

Allowed:

•**syslog** This format is for plain text files in a syslog-like format. It can also be used when there is no support for the logging format, and the logs are single line messages.

•**snort-full** This is used for Snort's full output format.

•**snort-fast** This is used for Snort's fast output format.

•squid

•iis

•**eventlog** This is used for Microsoft Windows eventlog format.

•**mysql_log** This is used for MySQL logs. It does not support multi-line logs.

•**postgresql_log** This is used for PostgreSQL logs. It does not support multi-line logs.

•**nmapg** This is used for monitoring files conforming to the grepable output from nmap.

•**apache**

This format is for apache's default log format.

Example:

•**command** This format will be the output from the command (as run by root) defined by command. Each line of output will be treated as a separate log.

•**full_command** This format will be the output from the commandi (as run by root) defined by command. The entire output will be treated as a single log.

Warning: `command` and `full_command` cannot be used in the agent.conf, and must be configured in each system's ospatrol.conf.

•djb-multilog

•**multi-line** This option will allow applications that log multiple lines per event to be monitored. This format requires the number of lines to be consistent. `multi-line:` is followed by the number of lines in each log entry. Each line will be combined with the previous lines until all lines are gathered. There may be multiple timestamps in a finalized event.

Allowed: <log_format>multi-line: NUMBER</log_format>

Example: Log messages:

```
Aug  9 14:22:47 hostname log line one
Aug  9 14:22:47 hostname log line two
Aug  9 14:22:47 hostname log line three
Aug  9 14:22:47 hostname log line four
Aug  9 14:22:47 hostname log line five
```

Log message as analyzed by **ospatrol-analysisd_**:

```
Aug  9 14:22:47 hostname log line one Aug  9 14:22:47 hostname log line two Aug  9
```

`command`

The command to be run. All output from this command will be read as one or more log messages depending on whether command or full_command is used.

Allowed: Any commandline and arguments.

`alias`

An alias to identify the command. This will replace the command in the log message.

For example `<alias>usb-check</alias>` would replace:

```
ospatrol: output: 'reg QUERY HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR':
```

with:

```
ospatrol: output: 'usb-check':
```

Allowed: Any string.

frequency
The minimum time in seconds between command runs. The command will probably not run every `frequency` seconds exactly, but the time between runs will not be shorter than this setting. This is used with command and full_command.

Allowed: Time in seconds.

check_diff
The output from an event will be stored in an internal database. Every time the same event is received, the output is compared to the previous output. If the output has changed an alert will be generated.

Monitoring logs

With in OSPatrol their is two major methods for monitoring logs: file and process. Each method has it's own page and examples.

Process Monitoring

Overview We love logs. Inside OSPatrol we treat everything as if it is a log and parse it appropriately with our rules. However, some information is not available in log files but we still want to monitor it. To solve that gap, we added the ability to monitor the output of commands via OSPatrol, and treat the output of those commands just like they were log files.

Configuration examples

Disk space utilization (df -h) example For example, if you wanted to monitor the disk space utilization, you would need to setup a cron job to dump the output of `df -h` to a log file (maybe /var/log/df.log) and configure OSPatrol to look at it.

As of OSPatrol version 2.3 you can monitor commands directly in OSPatrol following configuration:

```
<localfile>
    <log_format>command</log_format>
    <command>df -h</command>
</localfile>
```

Since we already have a sample rule for df -h included with OSPatrol you would see the following when any partition reached 100%:

```
** Alert 1257451341.28290: mail - ospatrol,low_diskspace,
2009 Nov 05 16:02:21 (home-ubuntu) 192.168.0.0->df -h

Rule: 531 (level 7) -> "Partition usage reached 100% (disk space monitor)."
Src IP: (none)
User: (none)
ospatrol: output: 'df -h': /dev/sdb1 24G 12G 11G 100% /var/backup
```

Load average (uptime) Example Another example, if you want to monitor the load average, you can configure OSPatrol to monitor the "uptime" command and alert when it is higher than 2, for example:

```
<localfile>
    <log_format>command</log_format>
    <command>uptime</command>
</localfile>
```

And in the rule:

```
<rule id="100101" level="7" ignore="7200">
    <if_sid>530</if_sid>
    <match>ospatrol: output: 'uptime': </match>
    <regex>load averages: 2.</regex>
    <description>Load average reached 2..</description>
</rule>
```

There are lots of possibilities with this feature. If you have ideas for commands to monitor and rules, please comment.

Alerting when output of a command changes If you want to create alerts when a log or the output of a command changes, take a look at the new <check_diff /> option in the rules (available on the latest snapshot).

To demonstrate with an example, we will create a rule to alert when there is a new port open in listening mode on our server.

First, we configure OSPatrol to run the `netstat -tan |grep LISTEN` command by adding the following to ospatrol.conf:

```
<localfile>
    <log_format>full_command</log_format>
    <command>netstat -tan |grep LISTEN|grep -v 127.0.0.1</command>
</localfile>
```

After that, I add a rule to alert when its output changes:

```
<rule id="140123" level="7">
    <if_sid>530</if_sid>
    <match>ospatrol: output: 'netstat -tan |grep LISTEN</match>
    <check_diff />
    <description>Listened ports have changed.</description>
</rule>'
```

Note that we use the `<check_diff />` option. The first time it receives the event, it will store in an internal database. Every time it receives the same event, it will compare against what we have store and only alert if the output changes.

In our example, after configuring OSPatrol, I started netcat to listen on port 23456 and that's the alert I got:

```
OSPatrol HIDS Notification.
2010 Mar 11 19:56:30

Received From: XYZ->netstat -tan |grep LISTEN|grep -v 127.0.0.1
Rule: 140123 fired (level 7) -> "Listened ports have changed."
Portion of the log(s):

ospatrol: output: 'netstat -tan |grep LISTEN|grep -v 127.0.0.1':
tcp4       0      0 *.23456              *.*                    LISTEN
tcp4       0      0 *.3306               *.*                    LISTEN
tcp4       0      0 *.25                 *.*                    LISTEN
Previous output:
ospatrol: output: 'netstat -tan |grep LISTEN|grep -v 127.0.0.1':
tcp4       0      0 *.3306               *.*                    LISTEN
tcp4       0      0 *.25                 *.*                    LISTEN
```

Detecting USB Storage Usage Xavier Mertens wrote a very interesting article on Detecting USB Storage Usage with OSPatrol. He used our policy auditing module for that, but I think USB monitoring can be done in a much easier way with our new `check_diff` feature.

To get started, first configure your Windows agents to monitor the USBSTOR registry entry using the reg command:

```
<agent_config os="windows">
    <localfile>
        <log_format>full_command</log_format>
        <command>reg QUERY HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR</command>
    </localfile>
</agent_config>
```

Next create a local rule for that command:

```
<rule id="140125" level="7">
    <if_sid>530</if_sid>
    <match>ospatrol: output: 'reg QUERY</match>
    <check_diff />
    <description>New USB device connected</description>
</rule>
```

Now after a few minutes you will see a directory at `/var/ospatrol/queue/diff/[agent_name]/[rule_id]` with the current snapshot of this command. Once someone adds a new USB device you will get this alert:

```
** Alert 1268687754.35062: mail  - local,syslog,
2010 Mar 15 18:15:54 (xx-netbook) any->reg QUERY HKLMSYSTEMCurrentControlSetEnumUSBSTOR
Rule: 140125 (level 7) -> 'New USB device connected'
Src IP: (none)
User: (none)
ospatrol: output: 'reg QUERY HKLMSYSTEMCurrentControlSetEnumUSBSTOR':! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTOR
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_&Prod_USB_Flash_Memory&Rev_5.00
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_Generic&Prod_Flash_Disk&Rev_8.0
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_Hitachi&Prod_HTS543225L9A300&Rev_
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_LEXAR&Prod_JD_FIREFLY&Rev_1100
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_SAMSUNG&Prod_HM160JC&Rev_0000
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_Sony&Prod_DSC&Rev_1.00
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_TomTom&Prod_ONE_XXL_IQ_Rts
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_USB_2.0&Prod_USB_Flash_Drive&Rev_0.00

Previous output:

ospatrol: output: 'reg QUERY HKLMSYSTEMCurrentControlSetEnumUSBSTOR':
! REG.EXE VERSION 3.0
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTOR
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_&Prod_USB_Flash_Memory&Rev_5.00
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_Generic&Prod_Flash_Disk&Rev_8.07
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_Hitachi&Prod_HTS543225L9A300&Rev_
HKEY_LOCAL_ACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_SAMSUNG&Prod_HM160JC&Rev_0000
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_Sony&Prod_DSC&Rev_1.00
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_TomTom&Prod_ONE_XXL_IQ_Rts
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTORDisk&Ven_USB_2.0&Prod_USB_Flash_Drive&Rev_0.00
```

File Monitoring

Overview OSPatrol has a process named ospatrol-logcollector that monitors log files for new events, and forwards them to other processes for analysis. The configuration of ospatrol-logcollector is done in `/var/ospatrol/etc/ospatrol.conf`.

Configuration examples

Simple example Configuring a log file to be monitored is simple. Just provide the name of the file to be monitored and the format:

```
<localfile>
    <location>/var/log/messages</location>
    <log_format>syslog</log_format>
</localfile>
```

Windows EventLog Example To monitor a Windows event log, you need to provide the format as "eventlog" and the location is the name of the event log. Example:

```
<localfile>
    <location>Security</location>
    <log_format>eventlog</log_format>
</localfile>
```

Multiple Files Example To check multiple files, OSPatrol supports posix regular expressions. For example, to analyze every file that ends with a .log inside the /var/log directory, use the following configuration:

```
<localfile>
    <location>/var/log/*.log</location>
    <log_format>syslog</log_format>
</localfile>
```

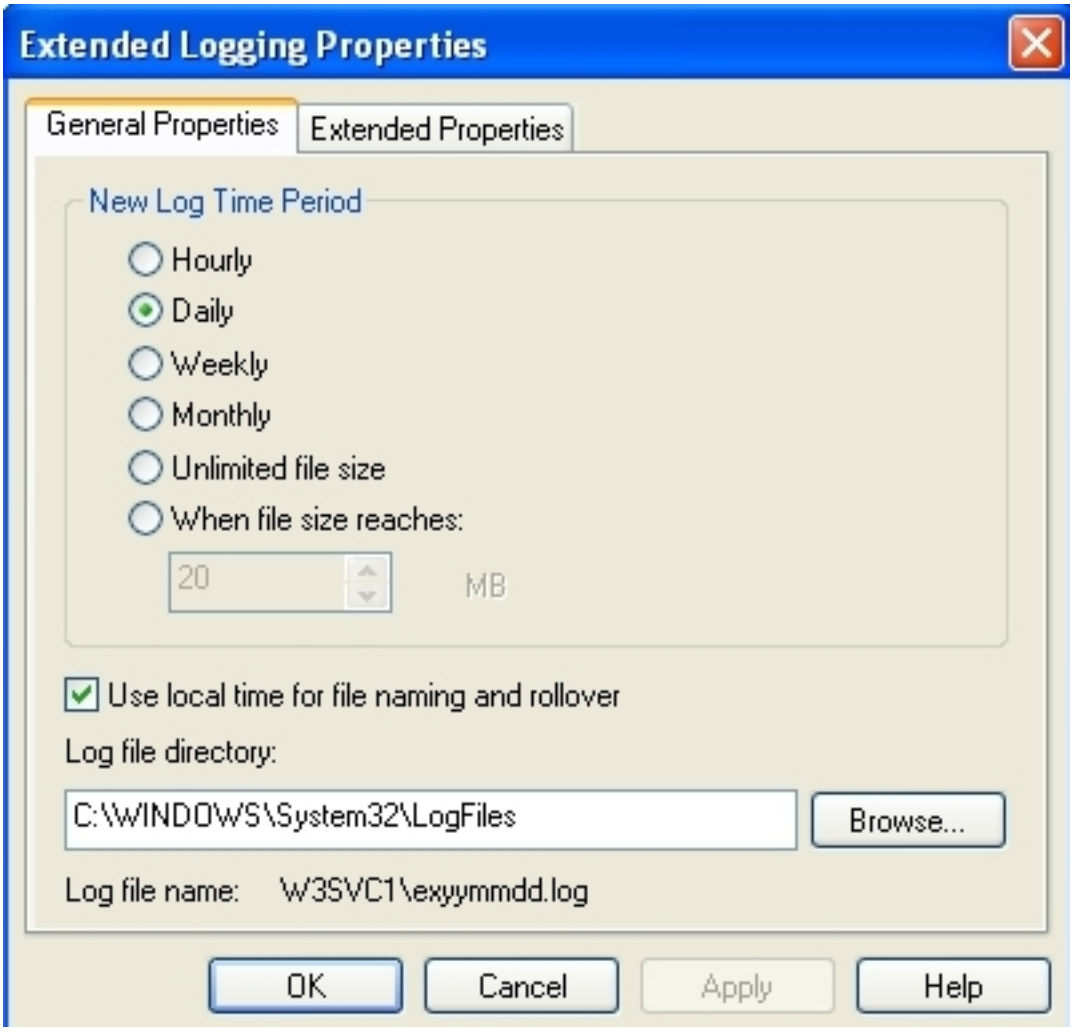
Date Based Example For log files that change according to the date, you can also specify a strftime format to replace the day, month, year, etc. For example, to monitor the log C:\Windows\app\log-08-12-15.log, where 08 is the year, 12 is the month and 15 the day (and it is rolled over every day), do:

```
<localfile>
    <location>C:\Windows\app\log-%y-%m-%d.log</location>
    <log_format>syslog</log_format>
</localfile>
```

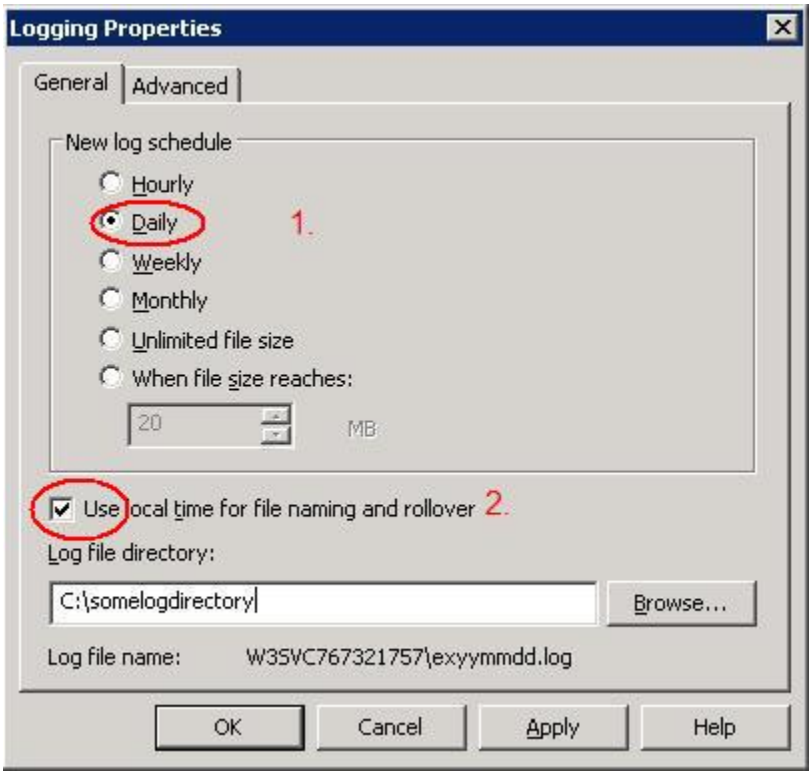
> **Warning:** Wildcards cannot be combined with the date based format.

IIS Logs Example Support for IIS (5 and 6) is available for the NCSA format (web only) and the W3C extended format (for Web, FTP and SMTP). By default, the installation scripts will attempt to configure OSPatrol to monitor the first virtual hosts for web (W3SVC1 to W3SVC254), ftp (MSFTPSVC1 to MSFTPSVC254) and smtp (SMTPSVC1 to SMTPSVC254). To monitor any other file you need to add a new entry manually.

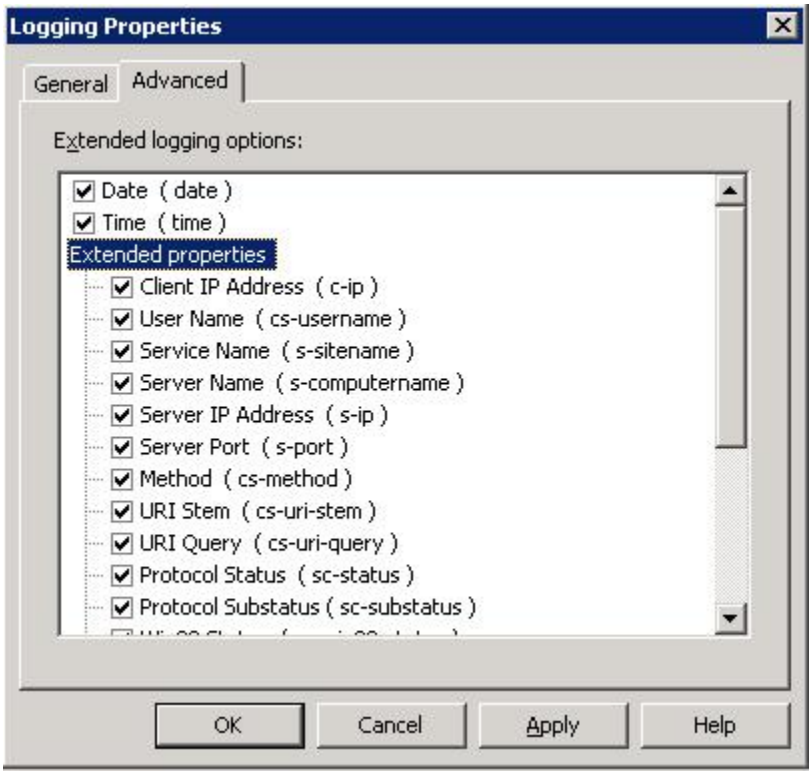
In addition to that, make sure to set the log time period to daily.



And using the local time for file naming and rollover.



In the extended logging properties, configure it to log the Date, Time and all the extended properties.



The following is an example of configuration to monitor the virtual server 2 of IIS web

```
<localfile>
    <location>%WinDir%\System32\LogFiles\W3SVC3\ex%y%m%d.log</location>
    <log_format>iis</log_format>
</localfile>
```

1.1.7 Syscheck

Syscheck is the name of the integrity checking process inside OSSEC. It runs periodically to check if any configured file (or registry entry on Windows) has changed.

Why Integrity checking?

This is the explanation from the OSSEC book:

> There are multiple types of attacks and many attack vectors, but there is one thing unique about all of them: they leave traces and always change the system in some way. From viruses that modify a few files, to kernel-level rootkits that alters the kernel, there is always some change in the integrity of the system.
>
> Integrity checking is an essential part of intrusion detection, that detects changes in the integrity of the system. OSSEC does that by looking for changes in the MD5/SHA1 checksums of the key files in the system and on the Windows registry.
>
> The way it works is that the agent scans the system every few hours (user defined) and send all the checksums to the server. The server stores the checksums and look for modifications on them. An alert is sent if anything changes.

Quick facts

- How often does it run?
  - By default every 6 hours, but the frequency or time/day are configurable.
- Where is the database stored?
  - On the manager in `/var/ossec/queue/syscheck`.
- How does it help with compliance? (PCI DSS, etc)
  - It helps with sections 11.5 (install FIM software) and 10.5 (integrity checking of log files) of PCI.
- How much CPU does it use?
  - The scans are performed slowly to avoid using too much CPU/memory.
- How are false positives handled?
  - Files can be ignored manually in the configuration or using rules. By default when a file has changed 3 times further changes are automatically ignored.

Realtime options

`ossec-syscheckd` is able to check file integrity in near realtime on Windows and modern Linux distros. Windows comes with support out of the box, but on Linux systems inotify packages may need to be installed. Check for inotify dev packages, and possibly an inotify-tools package.

Configuration options

These configuration options can be specified in each agent's ossec.conf file, except for the `auto_ignore` and `alert_new_file` which apply to manager and local installs. The `ignore` option applies to all agents if specified on the manager.

Configuration Examples

To configure syscheck, a list of files and directories must be provided. The check_all option checks md5, sha1, owner, and permissions of the file.

Example:

```
<syscheck>
    <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
    <directories check_all="yes">/root/users.txt,/bsd,/root/db.html</directories>
</syscheck>
```

Files and directories can be ignored using the `ignore` option (or `registry_ignore` for Windows registry entries):

```
<syscheck>
    <ignore>/etc/random-seed</ignore>
    <ignore>/root/dir</ignore>
    <ignore type="sregex">.log$|.tmp</ignore>
</syscheck>
```

The `type` attribute can be set to sregex to specify a *Regular Expression Syntax* in the ignore option.

```
<syscheck>
    <ignore type="sregex">^/opt/application/log</ignore>
</syscheck>
```

A local rule can be used to modify the severity for changes to specific files or directories:

```
<rule id="100345" level="12">
    <if_matched_group>syscheck</if_matched_group>
    <match>/var/www/htdocs</match>
    <description>Changes to /var/www/htdocs - Critical file!</description>
</rule>
```

In the above example, a rule was created to alert with high severity (12) for changes to the files in the htdocs directory.

Real time Monitoring

OSSEC supports realtime (continuous) file integrity monitoring on Linux (support was added kernel version 2.6.13) and Windows systems.

The configuration is very simple. In the `<directories>` option where you specify what directories to monitor, adding `realtime="yes"` will enable it. For example:

```
<syscheck>
    <directories realtime="yes" check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
    <directories check_all="yes">/bin,/sbin</directories>
</syscheck>
```

In this case, the directories /etc, /usr/bin and /usr/sbin will be monitored in real time. The same applies to Windows too.

Warning: The real time monitoring will not start immediately. First ossec-syscheckd needs to scan the file system and add each sub-directory to the realtime queue. It can take up to 30 minutes for this to finish (wait for the log "ossec-syscheckd: INFO: Starting real time file monitoring").

Note: Real time only works with directories, not individual files. So you can monitor the /etc or C:\program files directory, but not an individual file like /etc/file.txt.

Note: Both rootcheck and syscheck runs on the same thread, so when rootcheck is running, the inotify events would get queued until it finishes.

Report Changes

OSSEC supports sending diffs when changes are made to text files on Linux and unix systems.

Configuring syscheck to show diffs is simple, add `report_changes="yes"` to the `<directories` option.

For example:

```
<syscheck>
    <directories report_changes="yes" check_all="yes">/etc</directories>
    <directories check_all="yes">/bin,/sbin</directories>
</syscheck>
```

Syscheck: FAQ

How to force an immediate syscheck scan?

Run agent control tool to perform a integrity checking immediately (option -a to run on all the agents and -u to specify an agent id)

```
# /var/ospatrol/bin/agent_control -r -a
# /var/ospatrol/bin/agent_control -r -u <agent_id>
```

For more information see the *agent_control* documentation.

How to tell syscheck not to scan the system when OSPatrol starts?

Set the option <scan_on_start> to "no" on ospatrol.conf

How to ignore a file that changes too often?

Set the file/directory name in the <ignore> option or create a simple local rule.

The following one will ignore files /etc/a and /etc/b and the directory /etc/dir for agents mswin1 and ubuntu-dns:

```
<rule id="100345" level="0" >
    <if_group>syscheck</if_group>
    <description>Changes ignored.</description>
    <match>/etc/a|/etc/b|/etc/dir</match>
    <hostname>mswin1|ubuntu-dns</hostname>
</rule>
```

Why does OSPatrol still scan a file even though it's been ignored?

No idea. So if there are some directories you do not want scanned at all, make sure they are not included in a `<directories>` configuration.

How to know when the syscheck scan ran?

Use the agent_control tool on the manager, to see this information.

More information see the *agent_control* documentation.

How to get detailed reporting on the changes?

Use the syscheck_control tool on the manager or the web ui for that.

More information see the *syscheck_control* documentation.

Syscheck not sending any file data to the server?

With ospatrol 1.3 and Fedora you may run into this problem:

You have named files you'd like ospatrol to monitor so you add:

```
<ospatrol_config>
    <syscheck>
        <directories check_all="yes">/var/named</directories>
```

to ospatrol.conf on the client. Fedora – at least as of version 7 – runs named in a chroot jail under /var/named/chroot. However, part of that chroot jail includes /var/named/chroot/proc. The contents of that directory are purely ephemeral; there is no value to checking their integrity. And, at least in ospatrol 1.3, your syscheck may stall trying to read those files.

The symptom is a syscheck database on the server that never grows beyond a file or two per restart of the client. The log monitoring continues to work, so you know it's not a communication issue, and you will often see a slight increase in syscheck database file size after the client has restarted (in one case about 20 minutes after). But the database will never be completely built; there will only be a couple files listed in datebase.

The solution is to add an ignore clause to ospatrol.conf on the client:

```
<ospatrol_config>
    <syscheck>
        <ignore>/var/named/chroot/proc</ignore>
```

Why aren't new files creating an alert?

By default OSPatrol does not alert on new files. To enable this functionlity, <alert_new_files> must be set to yes inside the <syscheck> section of the manager's ospatrol.conf. Also, the rule to alert on new files (rule 554) is set to level 0 by default. The alert level will need to be raised in order to see the alert. Alerting on new files does not work in realtime, a full scan will be necessary to detect them.

Add the following to local_rules.xml:

```
<rule id="554" level="10" overwrite="yes">
  <category>ospatrol</category>
  <decoded_as>syscheck_new_entry</decoded_as>
  <description>File added to the system.</description>
  <group>syscheck,</group>
</rule>
```

The <alert_new_files> entry should look something like this:

```
<syscheck>
  <frequency>7200</frequency>
  <alert_new_files>yes</alert_new_files>
  <directories check_all="yes">/etc,/bin,/sbin</directories>
</syscheck>
```

Can OSPatrol include information on who changed a file in the alert?

In short, no. OSPatrol does not track this information. You could use your OS's auditing facilities to track this information, and create a rule to alert when an appropriate log is created.

1.1.8 Rootcheck Manual

Rootcheck

OSSEC HIDS will perform rootkit detection on every system where the agent is installed. The rootcheck (rootkit detection engine) will be executed every X minutes (user specified - by default every 2 hours) to detect any possible rootkit installed. Used with the log analysis and the integrity checking engine, it will become a very powerful monitoring solution.

Checks that rootcheck preforms

1. Read the rootkit_files.txt which contains a database of rootkits and files commonly used by them. It will try to stats, fopen and opendir each specified file. We use all these system calls because some kernel-level rootkits hide files from some system calls. The more system calls we try, the better the detection. This method is more like an anti-virus rule that needs to be updated constantly. The chances of false-positives are small, but false negatives can be produced by modifying the rootkits.

2. Read the rootkit_trojans.txt which contains a database of signatures of files trojaned by rootkits. This technique of modifying binaries with trojaned versions was commonly used by most of the popular rootkits available. This detection method will not find any kernel level rootkit or any unknown rootkit.
3. Scan the /dev directory looking for anomalies. The /dev should only have device files and the Makedev script. A lot of rootkits use the /dev to hide files. This technique can detect even non-public rootkits.
4. Scan the whole filesystem looking for unusual files and permission problems. Files owned by root, with write permission to others are very dangerous, and the rootkit detection will look for them. Suid files, hidden directories and files will also be inspected.
5. Look for the presence of hidden processes. We use getsid() and kill() to check if any pid is being used or not. If the pid is being used, but "ps" can't see it, it is the indication of kernel-level rootkit or a trojaned version of "ps". We also verify that the output of kill and getsid are the same.
6. Look for the presence of hidden ports. We use bind() to check every tcp and udp port on the system. If we can't bind to the port (it's being used), but netstat does not show it, we probably have a rootkit installed
7. Scan all interfaces on the system and look for the ones with "promisc" mode enabled. If the interface is in promiscuous mode, the output of "ifconfig" should show that. If not, we probably have a rootkit installed.

Configuration options

These configuration options can be specified in each agent's ossec.conf, except `auto_ignore` and `alert_new_file` which are manager side options. If the `ignore` option is specified on the manager the setting becomes global for all agents.

Understanding the Unix policy auditing on OSSEC

OSSEC's policy monitor allows you to verify that all your systems conform to a set of policies regarding configuration settings and applications usage. They are configured centrally on the ossec server and pushed down to the agents. It also checks if a system in in compliance with the CIS Security Benchmarks and VMware security hardening guidelines.

The following systems are tested for the CIS and VMware guidelines:

- Debian and Ubuntu
- Red Hat and Fedora
- Red Hat Enterprise Linux 5
- VMWare ESX 3.0 and 3.5

Receiving Audit and Application alerts via Email

By default, both the policy auditing and application checks are logged as level `3`, so you will not receive any e-mail alerts with the original configuration.

If you wish to receive e-mail alerts for any (or both of the two) types of events, you need to create local rules with a higher severity or with the `alert_by_email` option set.

Example1: Sending e-mail for every Audit event

Add to your local_rules.xml the following:

```
<pre>
  <rule id="512" level="9" overwrite="yes">
    <if_sid>510</if_sid>
    <match>^System Audit</match>
    <description>System Audit event.</description>
    <group>rootcheck,</group>
  </rule>
</pre>
```

Listing entries per agent

To control the policy database, use the ‘‘rootcheck_control’’ tool.

This page was originally authored by Daniel Cid for the OSSEC wiki.

1.1.9 Rules and Decoders

Testing OSSEC rules/decoders

The first problem most people have when troubleshooting OSSEC or trying to write new rules and decoders is how to test them. In the past, this would require manually restarting OSSEC or creating a testing installation. As of version 1.6, there is a tool to simplify this task (ossec-testrule).

Testing using ossec-logtest

The tool *ossec-logtest* is installed into `/var/ossec/bin`. It will read the current rules and decoder (from `/var/ossec`) and accept log input from stdin:

```
# /var/ossec/bin/ossec-logtest
2008/07/04 09:57:28 ossec-testrule: INFO: Started (pid: 12683).
ossec-testrule: Type one log per line.

Jul 4 09:42:16 enigma sshd[11990]: Accepted password for dcid from 192.168.2.10 port 35259 ssh2

**Phase 1: Completed pre-decoding.
full event: "Jul 4 09:42:16 enigma sshd[11990]: Accepted password for dcid from 192.168.2.10 port 352
hostname: "enigma"
program_name: "sshd"
log: "accepted password for dcid from 192.168.2.10 port 35259 ssh2"

**Phase 2: Completed decoding.
decoder: 'sshd'
dstuser: 'dcid'
srcip: '192.168.2.10

**Phase 3: Completed filtering (rules).
Rule id: '10100
Level: '4
Description: 'First time user logged in.'
**Alert to be generated.
```

In the above example, we provided an authentication success log and ossec-logtest showed us how it would be decoded, what information was extracted and which rule fired. In the next example, we can see how it would extract a user logoff message from Windows:

```
# /var/ossec/bin/ossec-logtest
2008/07/04 09:57:28 ossec-testrule: INFO: Started (pid: 12683).
ossec-testrule: Type one log per line.

WinEvtLog: Security: AUDIT_SUCCESS(538): Security: lac: OSSEC-HM: OSSEC-HM: User Logoff: User Name: l

**Phase 1: Completed pre-decoding.
full event: 'WinEvtLog: Security: AUDIT_SUCCESS(538): Security: lac: OSSEC-HM: OSSEC-HM: User Logoff
hostname: 'enigma'
program_name: '(null)'
log: 'WinEvtLog: Security: AUDIT_SUCCESS(538): Security: lac: OSSEC-HM: OSSEC-HM: User Logoff: User N

**Phase 2: Completed decoding.
decoder: 'windows'
status: 'AUDIT_SUCCESS'
id: '538
extra_data: 'Security'
dstuser: 'lac'
system_name: 'OSSEC-HM'

**Phase 3: Completed filtering (rules).
Rule id: '18149
Level: '3
Description: 'Windows User Logoff.'
**Alert to be generated.
```

In addition to the information above, *ossec-logtest -f* can be used to follow the log through the rule path:

```
# /var/ossec/bin/ossec-logtest -f
2008/07/04 10:05:43 ossec-testrule: INFO: Started (pid: 23007).
ossec-testrule: Type one log per line.

Jul 4 10:05:30 enigma sshd[27588]: Failed password for invalid user test2 from 127.0.0.1 port 19130 s

**Phase 1: Completed pre-decoding.
full event: 'Jul 4 10:05:30 enigma sshd[27588]: Failed password for invalid user test2 from 127.0.0.1
hostname: 'enigma'
program_name: 'sshd'
log: 'Failed password for invalid user test2 from 127.0.0.1 port 19130 ssh2

**Phase 2: Completed decoding.
decoder: 'sshd'
srcip: '127.0.0.1

**Rule debugging:
Trying rule: 1 - Generic template for all syslog rules.
*Rule 1 matched.
*Trying child rules.
Trying rule: 5500 - Grouping of the pam_unix rules.
Trying rule: 5700 - SSHD messages grouped.
*Rule 5700 matched.
*Trying child rules.
Trying rule: 5709 - Useless SSHD message without an user/ip.
Trying rule: 5711 - Useless SSHD message without a user/ip.
Trying rule: 5707 - OpenSSH challenge-response exploit.
Trying rule: 5701 - Possible attack on the ssh server (or version gathering).
Trying rule: 5706 - SSH insecure connection attempt (scan).
Trying rule: 5713 - Corrupted bytes on SSHD.
```

```
Trying rule: 5702 - Reverse lookup error (bad ISP or attack).
Trying rule: 5710 - Attempt to login using a non-existent user
*Rule 5710 matched.
*Trying child rules.
Trying rule: 5712 - SSHD brute force trying to get access to the system.

**Phase 3: Completed filtering (rules).
Rule id: '5710
Level: '5
Description: 'Attempt to login using a non-existent user'
**Alert to be generated.
```

CDB List lookups from within Rules

Allow for CDB lookups from within rules in OSSEC (ossec-analysisd) of all possible fields.

Use cases

Anything that has a large number of items. Some examples:

- named with recursive logs checking the www.malwaredomains.com list for suspicious domains
- lists of approved users by server
- mstark (on irc) originally came up with suggestion for approved software based on a md5 list
- IP address lookups - there are a large number of lists of suspicious or known bad IP addresses to match inside of ossec rules

Syntax for Lists

Rules A rule would use the following syntax to look up a key within a CDB database.

Positive key match This example is a search for the key within the `rules/cdb_record_file` and will match if they key is present:

```
<list field="program_name" lookup="match_key">rules/records</list>
```

The `lookup="match_key"` is the default and can be left out as in this example:

```
<list field="program_name">rules/records</list>
```

Negative key match This example is a search for the key stored in field attribute and will match if it *IS NOT* present in the database:

```
<list field="program_name" lookup="not_match_key">rules/records</list>
```

Key and Value match This example is a search for a key stored in the field attribute, and on a positive match the returned value of the key will be processed using the regex in the check_value attribute:

```
<list field="program_name" lookup="match_key_value" check_value="^reject">rules/records</list>
```

Positive IP address match This example is a search for the IP address stored in the field attribute and will match if it *IS* present in the database.

```
<list field="srcip" lookup="address_match_key">rules/records</list>
```

Negative IP address match This example is a search for the IP address stored in the field attribute and will match if it *IS NOT* present in the database.

```
<list field="srcip" lookup="not_address_match_key">rules/records</list>
```

Key and Value Address Match This example is a search for a key stored in the field attribute, and on a positive match the returned value of the key will be processed using the regex in the check_value attribute:

```
<list field="srcip" lookup="address_match_key_value" check_value="^reject">rules/records</list>
```

ossec.conf Each list will need to be defined and told to be available using the ossec.conf file. Using the following syntax:

```
<ossec_config>
    <rules>
        <list>rules/records</list>
```

Commands CDB files must be compiled before they can be used. *ossec-makelists* is used to compile lists.

The command *ossec-makelists* will process and compile all lists if the master text rules have been changed. Basicly logic is as follows:

- Read ossec.conf for all lists
- Check the mtime of each list and compare it to the mtime of the compiled .cdb file
- if mtime is newer create new database file ending in .tmp
- use atomic rename to change the .tmp to .cdb. This will invalidate all mmap pages currently in use by ossec-analysisd and will cause them to be reloaded with the new data as needed

List text file format Creating cdb lists the following file format is specified:

```
key1:value
key2:value
key3:diff value
```

Each key must be unique and is terminated with a colon `:`.

For IP addresses the dot notation is used for subnet matches

```
key         CIDR             Possible matches
10.1.1.1    10.1.1.1/32      10.1.1.1
192.168.    192.168.0.0/16   192.168.0.0 - 192.168.255.255
172.16.19.  172.16.19.0/24   172.16.19.0 - 172.16.19.255
```

Due to address lookups being based on the class boundary extra scripts are suggested for creating lists that need fine control. Example of IP address list file:

```
192.168.: RFC 1918 Address space
172.16.:RFC 1918 Address space
172.17.:RFC 1918 Address space
172.18.:RFC 1918 Address space
172.19.:RFC 1918 Address space
172.20.:RFC 1918 Address space
172.21.:RFC 1918 Address space
172.22.:RFC 1918 Address space
172.23.:RFC 1918 Address space
172.24.:RFC 1918 Address space
172.25.:RFC 1918 Address space
172.26.:RFC 1918 Address space
172.27.:RFC 1918 Address space
172.28.:RFC 1918 Address space
172.29.:RFC 1918 Address space
172.30.:RFC 1918 Address space
172.31.:RFC 1918 Address space
10.:RFC 1918 Address space
```

Note: Previous versions of this page page orginally was created by @j_hen on her blog http://jentalkstoomuch.blogspot.com/2010/09/writing-custom-ossec-rules-for-your.html Some content may be the same, but examples have been updated.

Note: In the xml based examples, any text between <!-- and --> are comments. In the console based examples, anything after # may be an example. For more information on OSSEC's non-standard regular expression (regex) syntax, refer to the regex page.

Create Custom decoder and rules

One of the main features of OSSEC is monitoring system and application logs. Many popular services have logs and decoders, but there are hundreds that are not covered. Custom applications and services will also not be covered. Adding decoders and rules for services is generally very easy.

Adding a File to be Monitored

Adding a log file to the configuration for monitoring is simple. In the system's ossec.conf add an entry like this:

```
<localfile>
  <log_format>syslog</log_format>
  <location>/path/to/log/file</location>
</localfile>
```

`syslog` is a generic format, consisting of a singular line of text appended to the log file. There are other formats available, they are detailed on the localfile syntax page.

Note: Additional examples can be found here. More detailed syntax can be found here.

After adding a localfile entry, the OSSEC processes must be restarted.

Create a Custom Decoder

The following log messages will be used for most of the examples in this section:

```
2013-11-01T10:01:04.600374-04:00 arrakis ossec-exampled[9123]: test connection from 192.168.1.1 via t
2013-11-01T10:01:05.600494-04:00 arrakis ossec-exampled[9123]: successful authentication for user tes
```

The first log message is broken down as follows:

- 2013-11-01T10:01:04.600374-04:00 - timestamp from rsyslog
- arrakis - hostname of the system
- ossec-exampled - daemon creating the log
- [9123] - process ID of the ossec-exampled instance
- test connection from 192.168.1.1 via test-protocol1 - log message

ossec-logtest will be used to test the custom decoder and any custom rules.

Custom decoders are added to the `local_decoder.xml` file, typically found in `/var/ossec/etc` on a standard installation. The basic syntax is listed here, but this page is not well documented at the moment.

Using ossec-logtest on this sample rule results in the following output:

```
# /var/ossec/bin/ossec-logtest
2013/11/01 10:39:07 ossec-testrule: INFO: Reading local decoder file.
2013/11/01 10:39:07 ossec-testrule: INFO: Started (pid: 32109).
ossec-testrule: Type one log per line.

2013-11-01T10:01:04.600374-04:00 arrakis ossec-exampled[9123]: test connection from 192.168.1.1 via t


**Phase 1: Completed pre-decoding.
       full event: '2013-11-01T10:01:04.600374-04:00 arrakis ossec-exampled[9123]: test connection fr
       hostname: 'arrakis'
       program_name: 'ossec-exampled'
       log: 'test connection from 192.168.1.1 via test-protocol1'

**Phase 2: Completed decoding.
       No decoder matched.
```

There is not a lot of output here because OSSEC does not understand this log. Creating a decoder for this log message will provide OSSEC much more information.

Phase 1 "pre-decodes" some information. The hostname is the system that generated the log message, program_name is the name of the application that created the log, and log is the rest of the log message.

The following is a very basic decoder for `ossec-exampled`:

```
<decoder name="ossec-exampled">
  <program_name>ossec-exampled</program_name>
</decoder>
```

This decoder simply looks for any log messages generated by `ossec-exampled`. Using a very generic decoder like this can allow an OSSEC user to create more specific child decoders for services with less consistant log messages.

Here is the ossec-logtest output after adding this decoder:

```
# /var/ossec/bin/ossec-logtest
2013/11/01 10:52:09 ossec-testrule: INFO: Reading local decoder file.
2013/11/01 10:52:09 ossec-testrule: INFO: Started (pid: 25151).
ossec-testrule: Type one log per line.

2013-11-01T10:01:04.600374-04:00 arrakis ossec-exampled[9123]: test connection from 192.168.1.1 via t
```

```
**Phase 1: Completed pre-decoding.
       full event: '2013-11-01T10:01:04.600374-04:00 arrakis ossec-exampled[9123]: test connection fr
       hostname: 'arrakis'
       program_name: 'ossec-exampled'
       log: 'test connection from 192.168.1.1 via test-protocol1'

**Phase 2: Completed decoding.
       decoder: 'ossec-exampled'
```

Phase 2 now correctly identifies this log message as coming from ossec-exampled. There is still some very important information in the log message that should be decoded, namely the source IP and `test-protocol1`. To decode these a child decoder will be added. It will set the `ossec-exampled` decoder as a parent, and use `prematch` to limit its use to the correct log message.

```
<decoder name="ossec-exampled-test-connection">
  <parent>ossec-exampled</parent>
  <prematch offset="after_parent">^test connection </prematch> <!-- offset="after_parent" makes OSSEC
  <regex offset="after_prematch">^from (\S+) via (\S+)$</regex> <!-- offset="after_prematch" makes OS
  <order>srcip, protocol</order>
</decoder>
```

Breaking this down piece by piece:

- `<decoder name="ossec-exampled-test-connection">` - Declaring this to be a decoder and giving it a name.
- `<parent>ossec-exampled</parent>` - This decoder will only be checked if `ossec-exampled` also matched.
- `<prematch offset="after_parent">^test connection </prematch>` - If a log message does not contain the data in the prematch, it will not use that decoder. Setting the offset tells OSSEC to only look at data after the parent (ossec-exampled[9123]: in this case), in an effort to speed up matches.
- `<regex offset="after_prematch">^from (\S+) via (\S+)$</regex>` - The regex line can be used to pull data out of the log message for use in rules. In this instance the first `\S+` matches the IP address, and the second matches the protocol. Anything between the parenthesis will be able to be used in rules.
- `<order>srcip, protocol</order>` - Defines what the entries in the regex line are labeled as. The IP address will be labeled as srcip, and the protocol by proto.

ossec-logtest output after adding this decoder:

```
# /var/ossec/bin/ossec-logtest
2013/11/01 11:03:25 ossec-testrule: INFO: Reading local decoder file.
2013/11/01 11:03:25 ossec-testrule: INFO: Started (pid: 6290).
ossec-testrule: Type one log per line.

2013-11-01T10:01:04.600374-04:00 arrakis ossec-exampled[9123]: test connection from 192.168.1.1 via t


**Phase 1: Completed pre-decoding.
       full event: '2013-11-01T10:01:04.600374-04:00 arrakis ossec-exampled[9123]: test connection fr
       hostname: 'arrakis'
       program_name: 'ossec-exampled'
       log: 'test connection from 192.168.1.1 via test-protocol1'

**Phase 2: Completed decoding.
       decoder: 'ossec-exampled'
```

```
       srcip: '192.168.1.1'
       proto: 'test-protocol1'
```

Note: The `decoder` will be labeled as the parent decoder, not the child. It's common to think a child decoder doesn't work because the parent decoder's name is listed, but that may not be a problem.

Now that the first sample log message is decoded, how does the second message fare? `ossec-logtest` output:

```
2013-11-01T10:01:05.600494-04:00 arrakis ossec-exampled[9123]: successful authentication for user tes


**Phase 1: Completed pre-decoding.
       full event: '2013-11-01T10:01:05.600494-04:00 arrakis ossec-exampled[9123]: successful authent
       hostname: 'arrakis'
       program_name: 'ossec-exampled'
       log: 'successful authentication for user test-user from 192.168.1.1 via test-protocol1'

**Phase 2: Completed decoding.
       decoder: 'ossec-exampled'
```

The decoded fields added in `ossec-exampled-test-connection` do not get decoded in this log message. This is expected because the `prematch` does not match. In this log message there are 4 fields that would be useful: status (successful), srcuser, srcip, and protocol. Adding a decoder for this should also be simple:

```
<decoder name="ossec-exampled-auth">
  <parent>ossec-exampled</parent>
  <prematch offset="after_parent"> authentication </prematch>
  <regex offset="after_parent">^(\S+) authentication for user (\S+) from (\S+) via (\S+)$</regex> <!
  <order>status, srcuser, srcip, protocol</order>
</decoder>
```

`ossec-logtest` output:

```
2013-11-01T10:01:05.600494-04:00 arrakis ossec-exampled[9123]: successful authentication for user tes


**Phase 1: Completed pre-decoding.
       full event: '2013-11-01T10:01:05.600494-04:00 arrakis ossec-exampled[9123]: successful authent
       hostname: 'arrakis'
       program_name: 'ossec-exampled'
       log: 'successful authentication for user test-user from 192.168.1.1 via test-protocol1'

**Phase 2: Completed decoding.
       decoder: 'ossec-exampled'
       status: 'successful'
       srcuser: 'test-user'
       srcip: '192.168.1.1'
       proto: 'test-protocol1'
```

Now the useful fields have been extracted for this log message as well. Double checking the original log message, to make sure there were no regressions:

```
2013-11-01T10:01:04.600374-04:00 arrakis ossec-exampled[9123]: test connection from 192.168.1.1 via t


**Phase 1: Completed pre-decoding.
       full event: '2013-11-01T10:01:04.600374-04:00 arrakis ossec-exampled[9123]: test connection fr
       hostname: 'arrakis'
```

```
       program_name: 'ossec-exampled'
       log: 'test connection from 192.168.1.1 via test-protocol1'

**Phase 2: Completed decoding.
       decoder: 'ossec-exampled'
       srcip: '192.168.1.1'
       proto: 'test-protocol1'
```

Directory path loading of rules and decoders

To allow whole directories of files to be loaded as decoders, lists, or rules by ossec-anaylistd.

Use case

Great simplifies working with decoders as their can be as many files as needed. Also will make packaging of rules and decoders a simple unzip/untar and restart operations. This will also greatly reduce the amount of code needed to manage the upgrade scripts of ossec.

Details

Syntax for OSSEC All Directory loading is done in alphabetical form. This is much like init.d where the use of numeric prefixes on file names can effect the order of loading. Example of file names and the order they would be loaded:

1. 00_sshd_rules.xml
2. 01_local_sshd_rules.xml
3. 99_shun_rules.xml

Directory loading The basic for selection of rules file is as follows. This will load all files in the rules dir that match the regex `_rules.xml$`

```
<ossec_config>
    <rules>
        <rule_dir pattern="_rules.xml">rules</rule_dir>
```

The pattern is optional and defaults to _rules.xml for rules loading so this could be writen as:

```
<ossec_config>
    <rules>
        <rule_dir>rules</rule_dir>
```

Order of the directives in ossec.conf is still respected, and duplicate files will not be loaded. In the following example 00_setup_rules.xml is always loaded first, and will *NOT* be loaded a second time by the rule_dir directive.

```
<ossec_config>
    <rules>
        <include>rules/00_setup_rules.xml</include>
        <rule_dir>rules</rule_dir>
```

For full details on all the Syntax see `rule_dir` and `decoder_dir`

Compete Examples of syntax This is an example where the decoders and rules have been broken out into subdirectories.

- rules/
  - 00_rules_config.xml
  - 50_apache_rules.xml
  - 50_arpwatch_rules.xml
  - plugins/
    - 50_wimax_rules.xml
    - 50_wimax_decoders.xml
- etc/
  - decoder.xml
  - local_decoder.xml

```
<ossec_config>
    <rules>
        <decoder>etc/decoder.xml</decoder>
        <decoder_dir>rules/plugins</decoder_dir>

        <rule>rules/rules/00_rules_config.xml</rule>
        <rule_dir pattern=".xml$">rules/</rule_dir>
        <rule_dir>rules/plugins</rule_dir>
    </rules>
</ossec_config>
```

Rules Classification

The rules are classified in multiple levels. From the lowest (00) to the maximum level 16. Some levels are not used right now. Other levels can be added between them or after them.

The rules will be read from the highest to the lowest level.

00 - Ignored - No action taken. Used to avoid false positives. These rulesare scanned before all the others. They include events with no security relevance.

01 - None -

02 - System low priority notification - System notification or status messages. They have no security relevance.

03 - Successful/Authorized events - They include successful login attempts, firewall allow events, etc.

04 - System low priority error - Errors related to bad configurations or unused devices/applications. They have no security relevance and are usually caused by default installations or software testing.

05 - User generated error - They include missed passwords, denied actions, etc. By itself they have no security relevance.

06 - Low relevance attack - They indicate a worm or a virus that have no affect to the system (like code red for apache servers, etc). They also include frequently IDS events and frequently errors.

07 - “Bad word” matching. They include words like “bad”, “error”, etc. These events are most of the time unclassified and may have some security relevance.

08 - First time seen - Include first time seen events. First time an IDS event is fired or the first time an user logged in. If you just started using OSSEC HIDS these messages will probably be frequently. After a while they should go away, It also includes security relevant actions (like the starting of a sniffer or something like that).

09 - Error from invalid source - Include attempts to login as an unknown user or from an invalid source. May have security relevance (specially if repeated). They also include errors regarding the "admin" (root) account.

10 - Multiple user generated errors - They include multiple bad passwords, multiple failed logins, etc. They may indicate an attack or may just be that a user just forgot his credencials.

11 - Integrity checking warning - They include messages regarding the modification of binaries or the presence of rootkits (by rootcheck). If you just modified your system configuration you should be fine regarding the "syscheck" messages. They may indicate a successful attack. Also included IDS events that will be ignored (high number of repetitions).

12 - High importancy event - They include error or warning messages from the system, kernel, etc. They may indicate an attack against a specific application.

13 - Unusual error (high importance) - Most of the times it matches a common attack pattern.

14 - High importance security event. Most of the times done with correlation and it indicates an attack.

15 - Severe attack - No chances of false positives. Immediate attention is necessary.

Rules Group

We can specify groups for specific rules. It's used for active response reasons and for correlation.

We currently use the following groups:

- invalid_login
- authentication_success
- authentication_failed
- connection_attempt
- attacks
- adduser
- sshd
- ids
- firewall
- squid
- apache
- syslog

1.1.10 Output and Alert options

Contents:

Sending alerts via syslog

Syslog output allows an OSSEC manager to send the OSSEC alerts to one or more syslog servers. OSSEC also supports sending alerts via cef, json, and to Splunk.

Configuration options

These configurations options require a server or local installation.

Enable Syslog output in the configuration

OSSEC can be configured to send the alerts via syslog to the servers of your choice. In this example all alerts are sent to 192.168.4.1, but only alerts of level 10 and above are sent to 10.1.1.1:

```
<syslog_output>
    <server>192.168.4.1</server>
</syslog_output>

<syslog_output>
    <level>10</level>
    <server>10.1.1.1</server>
</syslog_output>
```

After this change is made, the client-syslog process should be enabled:

```
# /var/ossec/bin/ossec-control enable client-syslog
```

And finally restart the OSSEC processes:

```
# /var/ossec/bin/ossec-control restart
```

ossec-csyslog should start along with the other OSSEC processes:

```
OSSEC HIDS v1.5.1 Stopped
Starting OSSEC HIDS v1.5.1 (by Third Brigade, Inc.)
Started ossec-csyslogd...
..
```

And in the logs:

```
# tail -n 1000 /var/ossec/logs/ossec.log | grep csyslog
2008/07/25 12:55:16 ossec-csyslogd: INFO: Started (pid: 19412).
2008/07/25 12:55:16 ossec-csyslogd: INFO: Forwarding alerts via syslog to: '192.168.4.1:514.
2008/07/25 12:55:16 ossec-csyslogd: INFO: Forwarding alerts via syslog to: '10.1.1.1:514.
```

This is what the syslog server should receive (every log separated by level, rule, location and the actual event that generated it):

```
Jul 25 12:17:41 enigma ossec: Alert Level: 3; Rule: 5715 - SSHD authentication success.; Location: (
srcip: 192.168.2.190; user: root; Jul 25 13:26:24 slacker sshd[20440]: Accepted password for root fr
```

Sending alerts via E-Mail

There are currently three types of email alerts:

- Single Notification E-Mail addresses
- Granular Notifications to any number of E-mail addresses
- Daily E-mail Reports

> **Warning:** Single E-Mail Notification must be setup before Granular Notification will work.

Alerts to a single E-Mail Address

In order to send notifications to a single address three items need to be setup within ossec.conf

Global E-Mail address destination The destination email address and mail host should be configured inside the <global> section of the /var/ossec/etc/ossec.conf.

```
<ossec_config>
    <global>
        <email_notification>yes</email_notification>
        <email_to>me@example.com</email_to>
        <smtp_server>mx.example.com..</smtp_server>
        <email_from>ossec@example.com</email_from>
```

Full details on all the options are avaiable at *ossec_config.global*

Set the alert levels that will send notifications The minimum email_alert_level can be set inside the <alerts> section of the /var/ossec/etc/ossec.conf file.

```
<ossec_config>
    <alerts>
        <email_alert_level>10</email_alert_level>
```

Full details on all the options are avaiable at *ossec_config.alerts*

Restart OSSEC to complete the changes OSSEC needs to be restarted for the change to take effect.

```
# /var/ossec/bin/ossec-control restart
```

Granular E-Mail alerts to many E-Mail addresses

OSSEC allows very granular options for the e-mail alerting and its format (full or SMS).

Note: Note that there must be at least one <email_to> recipient mentioned in the <global> section of the configuration or no emails will be sent at all.

Example 1: Group alerts If you want to e-mail *xx@y.z* for every event in the group syslog you can add the following to ossec

```
<email_alerts>
    <email_to>xx@y.z</email_to>
    <group>syslog</group>
</email_alerts>
```

Example 2: Message Format To e-mail (in the SMS format) *aa@y.z* for every event with severity higher than 10

Note: Note that the SMS format is not grouped, so the e-mail is sent immediately).

```
<email_alerts>
    <email_to>aa@y.z</email_to>
    <level>10</level>
    <format>sms</format>
</email_alerts>
```

Example 3: Email based on Rule ID's To e-mail *bb@y.z* for every event from rule 123 or rule 124 (without grouping):

Example 4: Email based on severity and agent To e-mail *cc@y.z* for every event with severity higher than 12, from agent qwert or agt1, without any delay (immediately):=====

```
<email_alerts>
    <email_to>cc@y.z</email_to>
    <level>12</level>
    <event_location>qwerty|agt1</event_location>
    <do_not_delay />
</email_alerts>
```

Example 5: Multiple granular options together You can have as many granular options as you want. In this example, we want the following:

- Email cc@y.z for every alert from agents qwerty and agt1
- Email john@y.z for every alert from agent secsys, lowsys and aixsys
- Email mike@y.z for every alert from /log/secure (from any agent)
- Email l@y.z for every alert from 192.168.0.0/24 network
- Email boss@y.z for every alert above level 10.

```
<ossec_config>
    <email_alerts>
        <email_to>cc@y.z</email_to>
        <event_location>qwerty|agt1</event_location>
    </email_alerts>

    <email_alerts>
        <email_to>john@y.z</email_to>
        <event_location>secsys|lowsys|aixsys</event_location>
    </email_alerts>

    <email_alerts>
        <email_to>mike@y.z</email_to>
        <event_location>/log/secure$</event_location>
    </email_alerts>

    <email_alerts>
        <email_to>l@y.z</email_to>
        <event_location>192.168.</event_location>
    </email_alerts>

    <email_alerts>
        <email_to>boss@y.z</email_to>
        <level>12</level>
```

```
    </email_alerts>
</ossec_config>
```

Daily E-Mail Reports

Daily E-Mail reports are summaries of the OSSEC alerts for the day.

Configuration options All of these configuration options should be specified in the /var/ossec/etc/ossec.conf.

Examples

Receive a summary of all authentication success alerts The following example will send a daily report of all authentication_success alerts, sorted by the related field srcip.

```
<ossec_config>
    <reports>
        <category>authentication_success</category>
        <user type="relation">srcip</user>
        <title>Daily report: Successful logins</title>
        <email_to>me@example.com</email_to>
```

Receive summary of all File integrity monitoring alerts The following example will send a report of all events related to syscheck.

```
<ossec_config>
    <reports>
        <category>syscheck</category>
        <title>Daily report: File changes</title>
        <email_to>me@example.com</email_to>
```

Sending output to a Database

OSSEC supports MySQL and PostgreSQL database outputs.

Configuration options

These configurations options can be specified in the server or local install ossec.conf file.

Enabling Database Support

Note: You must have the MySQL or PgSQL Client libraries installed on the OSSEC server.

Before you run the "./install.sh" script execute the following to compile OSSEC with database support.

```
# cd ossec-hids-*
# cd src; make setdb; cd ..
# ./install.sh
```

Enable Database output in the configuration

After installation is complete database support needs to be enabled. The following command will enable the database daemon on the next restart.

```
# /var/ossec/bin/ossec-control enable database
```

Database Specific Setup

Configuring MySQL

Database Setup Create a database, setup the database user, and add the schema (located in the `src/os_dbd` directory of the distribution) with the following commands.

```
# mysql -u root -p

mysql> create database ossec;

mysql> grant INSERT,SELECT,UPDATE,CREATE,DELETE,EXECUTE on ossec.* to ossecuser@<ossec ip>;
Query OK, 0 rows affected (0.00 sec)

mysql> set password for ossecuser@<ossec ip>=PASSWORD('ossecpass');
Query OK, 0 rows affected (0.00 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> quit

# mysql -u root -p ossec < mysql.schema
```

OSSEC Setup In order for ossec to output alerts and other data into the database the /var/ossec/etc/ossec.conf will need to have a <database_output> section added.

```
<ossec_config>
    <database_output>
        <hostname>192.168.2.30</hostname>
        <username>ossecuser</username>
        <password>ossecpass</password>
        <database>ossec</database>
        <type>mysql</type>
    </database_output>
</ossec_config>
```

The values will need to be corrected for your installations hostname, mysql user, password, and database.

Complete MySQL Output All that is left is to enable the database daemon and restart ossec for the changes to take effect.

```
# /var/ossec/bin/ossec-control enable database
# /var/ossec/bin/ossec-control restart
```

Configuring PgSQL

Database Setup Create a user for OSSEC within PgSQL

```
$ sudo -u postgres createuser -D -A -P ossec_user
Enter password for new role:
Enter it again:
Shall the new role be allowed to create more new roles? (y/n) n
CREATE ROLE
```

Create a database for OSSEC

```
$ sudo -u postgres createdb -O ossec_user ossecdb
CREATE DATABASE
```

Create the necessary tables from the PostgreSQL schema located in the `src/os_dbd` directory of the distribution.

```
$ psql -h 127.0.0.1 -U ossec_user -d ossecdb -f postgresql.schema
```

OSSEC Setup In order for ossec to output alerts and other data into the database the /var/ossec/etc/ossec.conf will need to be updated and a <database_output> section will need to be added.

```
<ossec_config>
    <database_output>
        <hostname>192.168.2.30</hostname>
        <username>ossecuser</username>
        <password>ossecpass</password>
        <database>ossec</database>
        <type>postgresql</type>
    </database_output>
</ossec_config>
```

The values will need to be corrected for your installation's hostname, postgresql user, password, and database.

Complete PgSQL Output All that is left is to enable the database daemon and restart ossec for the changes to take effect.

```
# /var/ossec/bin/ossec-control enable database
# /var/ossec/bin/ossec-control restart
```

Sending output to prelude

Prelude is a Hybrid IDS that uses IDMEF to receive alert information from external devices. If you are a Prelude user and wish to send your OSSEC alerts to Prelude, do the following:

Enabling Prelude Support

Note: You must have the Prelude libraries installed on the OSSEC server.

Before you run the "./install.sh" script execute the following to compile OSSEC with prelude support.

```
# cd ossec-hids-*
# cd src; make setprelude; cd ..
# ./install.sh
```

Enable Prelude output in the configuration

Just add the following entry to your ossec.conf inside the <global> section.

```
<prelude_output>yes</prelude_output>
```

Prelude extra options

You can define your own profile and set the log level from which you can send alerts to prelude with those parameters. Once again in the <global> section.

```
<prelude_profile>MyOssecProfile</prelude_profile>
<prelude_log_level>6</prelude_log_level>
```

Sending alerts to picviz

Warning: PicViz support is experimental, and not fully supported. Bug reports and improvements are needed.

Installation of PicViz

This is out of the scope for this document, but the development version from svn is required for PicViz to work with OSSEC.

Setup OSSEC for PicViz

Configure OSSEC to send events to PicViz. The following configuation needs to be added to /var/ossec/etc/ossec.conf.

```
<ossec_config>
    <global>
        <picviz_output>yes</picviz_output>
        <picviz_socket>/var/ossec/picviz.socket</picviz_socket>
```

For more full details on this section of the config see *ossec_config.global*.

Start up PicViz

On the picviz side, an OSSEC template is available in the template directory and Picviz should be run like this:

```
# pcv -Tpngcairo -o ossec.png -s /var/ossec/picviz.socket -t templates/ossec.pgdt -a
```

1.1.11 Active Response

The Active Response feature within OSPatrol can run applications on an agent or server in response to certain triggers. These triggers can be specific alerts, alert levels, or rule groups.

The active response framework is also what allows an OSPatrol administrator to start a syscheck scan or restart OSPatrol on a remote agent.

Creating Customized Active Responses

OSPatrol by default comes with a few active response scripts, but if you ever need to expand them, this tutorial can be of help.

As always, learning via examples is easier and faster. We will write a simple active response script to e-mail the alert to a specific address.

Creating the command

The first thing we need to do is to create a new "command" entry in the ospatrol config.

```
<command>
    <name>mail-test</name>
    <executable>mail-test.sh</executable>
    <timeout_allowed>no</timeout_allowed>
    <expect />
</command>
```

Since our script does not need a timeout, we set it to no. We also don't expect any input (like srcip or username), so we leave the "expect" tag empty. In the executable tag, we specify the name of the script to be executed (it must be inside /var/ospatrol/active-response/bin/).

Note: If you do need a srcip or username, just add it, eg: <expect>srcip</expect>

Configure the Active response

Next, we need to configure ospatrol to run the active response. In my case, I want to run it on the ospatrol server (so I choose location server) and every time the rule 1002 is fired (see rules_id 1002). You can also specify the level or different locations.

```
<active-response>
    <command>mail-test</command>
    <location>server</location>
    <rules_id>1002</rules_id>
</active-response>
```

Create active response script

With that done, we can create the active response script. The mail-test.sh must be inside the /var/ospatrol/active-response/bin/ with the execution permissions set.

What are the arguments are passed to the script?

1. action (delete or add)
2. user name (or - if not set)
3. src ip (or - if not set)
4. Alert id (uniq for every alert)
5. Rule id
6. Agent name/host/filename

```
#!/bin/sh
# E-mails an alert - copy at /var/ospatrol/active-response/bin/mail-test.sh
# Change e-mail ADDRESSS
# Author: Daniel Cid

MAILADDRESS="xx@ospatrol.net"
ACTION=$1
USER=$2
IP=$3
ALERTID=$4
RULEID=$5

LOCAL=`dirname $0`;
cd $LOCAL
cd ../
PWD=`pwd`


# Logging the call
echo "`date` $0 $1 $2 $3 $4 $5 $6 $7 $8" >> ${PWD}/../logs/active-responses.log


# Getting alert time
ALERTTIME=`echo "$ALERTID" | cut -d  "." -f 1`

# Getting end of alert
ALERTLAST=`echo "$ALERTID" | cut -d  "." -f 2`

# Getting full alert
grep -A 10 "$ALERTTIME" ${PWD}/../logs/alerts/alerts.log | grep -v ".$ALERTLAST: " -A 10 | mail $MAI
```

Restart OSPatrol and test

After the configuration is done, you can restart OSPatrol and test the configuration. For thee above example, I can run the logger command to similar a segmentation fault message.

```
# /var/ospatrol/bin/ospatrol-control restart
# logger "Segmentation Fault"
```

You should get in the /var/ospatrol/logs/active-response.log, the following:

```
Fri Jul 27 23:48:31 BRT 2007 /var/ospatrol/active-response/bin/mail-test.sh add - - 1185590911.25916
```

And in your e-mail:

```
from: root <root@xx.org>
to: xx@ospatrol.net
date: Jul 27,27 2007 11:48 PM
subject: OSPatrol Alert

** Alert 1185590911.25661: mailsl  - syslog,errors,
2007 Jul 27 23:48:31 xx->/var/log/messages
Rule: 1002 (level 7) -> 'Unknown problem somewhere in the system.'
Src IP: (none)
User: (none)
Jul 27 23:48:30 xx dcid: Segmentation Fault 123
```

UNIX: Active Response Configuration

The Active response configuration is divided into two parts. In the first one you configure the commands you want to execute. In the second one, you bind the commands to rules or events.

Commands Configuration

In the commands configuration you create new "commands" to be used as responses. You can have as many commands as you want. Each one should be inside their own "command" element. You can see an example here (for the host-deny.sh) and one here (for disable-account.sh).

```
<command>
    <name>The name (A-Za-Z0-9)</name>
    <executable>The command to execute (A-Za-z0-9.-)</executable>
    <expect>Comma separated list of arguments (A-Za-z0-9)</expect>
    <timeout_allowed>yes/no</timeout_allowed>
</command>
```

- **name**: Used to link the command to the response.
- **executable**: It must be a file (with exec permissions) inside "/var/ospatrol/active-response/bin".

  You don't need to provide the whole path.
- **expect**: The arguments this command is expecting (options are srcip and username).
- **timeout_allowed**: Specifies if this command supports timeout.

Responses Configuration

In the active-response configuration, you bind the commands (created) to events. You can have as many responses as you want. Each one should be inside their own "active-response" element. Examples are here (for blocking based on the severity) and here (for blocking on specific rules).

In the active-response configuration, you bind the commands (created) to events. You can have as many responses as you want. Each one should be inside their own "active-response" element. Examples are here (for blocking based on the severity) and here (for blocking on specific rules).

```
<active-response>
    <disabled>Completely disables active response if "yes"</disabled>
    <command>The name of any command already created</command>
    <location>Location to execute the command</location>
    <agent_id>ID of an agent (when using a defined agent)</agent_id>
    <level>The lower level to execute it (0-9)</level>
    <rules_id>Comma separated list of rules id (0-9)</rules_id>
    <rules_group>Comma separated list of groups (A-Za-z0-9)</rules_group>
    <timeout>Time to block</timeout>
</active-response>
```

- **disabled**: Disables active response if set to yes.
- **command**: Used to link the response to the command
- **location**: Where the command should be executed. You have four options:
  - **local**: on the agent that generated the event
  - **server**: on the OSPatrol server
  - **defined-agent**: on a specific agent (when using this option, you need to set the agent_id to use)

  - **all**: or everywhere.
- **agent_id**: The ID of the agent to execute the response (when defined-agent is set).
- **level**: The response will be executed on any event with this level or higher.
- **timeout**: How long until the reverse command is executed (IP unblocked, for example).

Active Response Tools

By default, the ospatrol hids comes with the following pre-configured active-response tools:

- **host-deny.sh**: Adds an IP to the /etc/hosts.deny file (most Unix systems).
- **firewall-drop.sh** (iptables): Adds an IP to the iptables deny list (Linux 2.4 and 2.6).
- **firewall-drop.sh** (ipfilter): Adds an IP to the ipfilter deny list (FreeBSD, NetBSD and Solaris).
- **firewall-drop.sh** (ipfw): Adds an IP to the ipfw deny table (FreeBSD).

  Note: On IPFW we use the table 1 to add the IPs to be blocked. We also set this table as deny in the beginning of the firewall list. If you use the table 1 for anything else, please change the script to use a different table id.

- **firewall-drop.sh** (ipsec): Adds an IP to the ipsec drop table (AIX).
- **firewall-drop.sh** (pf): Adds an IP to a pre-configured pf deny table (OpenBSD and FreeBSD).

  Note: On PF, you need to create a table in your config and deny all the traffic to it. Add the following lines at the beginning of your rules and reload pf (pfctl -F all && pfctl -f /etc/pf.conf): table <ospatrol_fwtable> persist #ospatrol_fwtable

  block in quick from <ospatrol_fwtable> to any block out quick from any to <ospatrol_fwtable>

Windows: Active Response Configuration

To start, you need to enable active response on Windows (disabled by default). To do that, just add the following to the agent's ospatrol.conf:

```
<active-response>
    <disabled>no</disabled>
</active-response>
```

After that, you need to go to the manager and specify when to run the response. Adding the following to ospatrol.conf will enable the responses for alerts above level 6:

```
<command>
    <name>win_nullroute</name>
    <executable>route-null.cmd</executable>
    <expect>srcip</expect>
    <timeout_allowed>yes</timeout_allowed>
</command>

<active-response>
    <command>win_nullroute</command>
    <location>local</location>
    <level>6</level>
```

```
    <timeout>600</timeout>
</active-response>
```

With the configuration completed (and the manager restarted), you can test the active response by running the agent-control script (in this case, I am running it on agent id 185 to block ip 2.3.4.5):

```
# /var/ospatrol/bin/agent_control -L

OSPatrol HIDS agent_control. Available active responses:

Response name: host-deny600, command: host-deny.sh
Response name: firewall-drop600, command: firewall-drop.sh
Response name: win_nullroute600, command: route-null.cmd

# /var/ospatrol/bin/agent_control -b 2.3.4.5 -f win_nullroute600 -u 185

OSPatrol HIDS agent_control: Running active response "win_nullroute600 "n: 185
```

And looking at the agent you should see the new entry in the route table:

```
C:\>route print
..
Active Routes:
Network Destination Netmask Gateway Interface Metric
2.3.4.5 255.255.255.255 x.y.z x.y.z 1
..
```

If you run into any issues, look at the ospatrol.log file (on the agent) for any entry for ospatrol-execd. If you enabled it correctly, you will see:

Understanding Active Response with FreeBSD

There are currently 3 options for firewalls in FreeBSD: IPF, IPFW, and PF. Each is configured differently on FreeBSD. OSPatrol will attempt to check for IPFW and then PF, falling back to IPF if neither of these was found at the time of installation.

How does OSPatrol know which firewall is being used?

The OSPatrol install script will check `rc.conf` to determine which firewall is currently active. It first greps for `firewall_enable="YES"`, and enables IPFW if this is found. IPFW support is enabled by copying the `ipfw.sh` to `/var/ospatrol/active-response/bin/firewall-drop.sh`. The installation script will then look for ‘‘pf_enable=”YES”‘ in the rc.conf, and will enable PF instead if this is found. The script for pf is pf.sh. If neither of these is found, the default firewall-drop.sh script will be installed. This script will use attempt to use IPF to block IPs.

How do I change which script is used by an agent?

Copy the appropriate script from the OSPatrol source to `/var/ospatrol/active-response/bin/firewall-drop.sh` on the agent.

1.2 Frequently asked questions

1.2.1 Agents: FAQ

Why can't agent IDs be re-used?

When looking at historical alerts you don't want to associate alerts from one system to be attributed to another, especially if the those alerts are from an unrelated and retired system.

1.2.2 Alerts: FAQ

How do you monitor for usb storage?

The first step is to configure the agents to check a registry entry with the `reg` command:

```
<agent_config os="Windows">
  <localfile>
    <log_format>full_command</log_format>
    <command>reg QUERY HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR</command>
    <alias>usb-check</alias>
  </localfile>
</agent_config>
```

Next create a local rule for that command:

```
<rule id="140125" level="7">
  <if_sid>530</if_sid>
  <match>ospatrol: output: 'usb-check':</match>
  <check_diff />
  <description>New USB device connected</description>
</rule>
```

When a USB drive is inserted into a Windows machine, an alert will not be triggered. The alert will contain a diff of the registry entry before the USB device was inserted and after.

Originally from: 'http://dcid.me/2010/03/detecting-usb-storage-usage-with-ospatrol/'

Additional data from: 'http://blog.rootshell.be/2010/03/15/detecting-usb-storage-usage-with-ospatrol/'

Why do I see alerts for agent2 in an email about agent1?

When an email is being prepared alerts will be grouped together. The only real criteria for grouping alerts together is the timeframe. To prevent alerts from being grouped together you can set `maild.groupping` to 0 in `/var/ospatrol/etc/internal_options.conf`. If this is set, alerts will be sent out individually. By default OSPatrol will only send 12 emails per hour. To increase this limit, modify or add the <email_maxperhour> setting in the `<global>` section of the `ospatrol.conf`. (see: email_maxperhour .)

Alerts for different sensors are appearing in the same email, how do I stop this from happening?

Read the previous FAQ entry.

How do I ignore rule 1002?

Rule 1002 is a catch-all rule. It looks for keywords that are generally considered "bad." It also means there is not currently a rule that deals with the log message. It is configured to always send an email when it's triggered, and many users have found it annoying. The best thing to do when you encounter something that triggers rule 1002 is write a rule. Contributing the logs and/or rules back to the project is also encouraged. Unless the application creating the log is an internal application, someone else may find the rule useful.

I set the <email_alert_level> to 10, why do I keep seeing rules with lower levels?

Some rules have an option set to force OSPatrol into sending an alert email. This option is `<options>alert_by_email</options>`. One of these rules is 1002. To ignore these rules you will have to create a rule to specifically ignore it, or overwrite the rule without the `alert_by_email` option.

1.2.3 OSPatrol: FAQ

Can an OSPatrol manager have more than 256 agents?

By default OSPatrol limits the number of agents to 256 per manager. This limitation is set in the code, but can be modified at compile time. Depending on the event load, a manager running on modern hardware can handle many more agents. Some users have more than 1000 agents on a single manager. To change the maximum number of agents, cd into the src directory and run the following command:

```
make setmaxagents
```

You should be prompted for the number of agents to allow.

One issue you may face after changing this setting is the number of files allowed to be open for a single user. The users `ospatrol` and `ospatrolr` both open at least 1 file (syscheck database and rids file) per agent. Raising this limit is operating system specific.

Some Linux distributions support a `/etc/security/limits.conf`. Set the limits to be at least a few files above what the max agents is set to.

```
ospatrol            soft    nofile          2048
ospatrol            hard    nofile          2048
ospatrolr           soft    nofile          2048
ospatrolr           hard    nofile          2048
```

Where are OSPatrol's logs stored?

On OSPatrol server and local installs there are several classes of OSPatrol logs. There are the logs created by the OSPatrol daemons, the log messages from the agents, and the alerts. Agent installs do not have logs from other agents or alerts, but do have logs created by the OSPatrol processes.

All logs are stored in subdirectories of `/var/ospatrol/logs`. OSPatrol's log messages are stored in `/var/ospatrol/logs/ospatrol.log`.

Log messages from the agents are not stored by default. After analysis they are deleted unless the <logall> option is included in the manager's ospatrol.conf. If set all log messages sent to the manager are stored in `/var/ospatrol/logs/archives/archives.log` and rotated daily.

Alerts are stored in `/var/ospatrol/logs/alerts/alerts.log`, and rotated daily.

Where can I view the logs sent to an OSPatrol manager (or on a local install)?

OSPatrol does not store the logs sent to it by default. If a log does not trigger an alert it is discarded, and logs that do trigger alerts are stored with the alerts in `/var/ospatrol/logs/alerts`.

The `<log-all>` option can be added to the `<global>` section (see: *ospatrol.conf: Global options*) of the manager's ospatrol.conf. The manager's OSPatrol processes should be restarted. The raw logs will then be saved to files, organized by date, in `/var/ospatrol/logs/archives`.

The headers attached to these log messages are in the format of `"YYYY Month dd HH:MM:ss agent_name->/path/to/log/file "`.

```
2011 Aug 04 00:00:01 server->/var/log/local7 Aug  4 00:00:26 server named[29909]: client 192.168
```

Can OSPatrol's logs be saved to a different directory?

As a protection mechanism, OSPatrol chroots most of its processes to the install directory (typically `/var/ospatrol`). Due to this chroot, logs must be saved to a location under `/var/ospatrol`. OSPatrol does rotate its logs, but will not be able to move them from `/var/ospatrol`.

Be sure to allocate enough space to `/var/ospatrol`.

I'm getting an error when starting OSPatrol: "OSPatrol analysisd: Testing rules failed. Configuration error. Exiting." Why?

There was a small bug in the ospatrol-control script that was not caught in time for 2.6. The error comes from the script trying to run ospatrol-logtest from the wrong directory. The solution is to change the line where ospatrol-logtest is running to look like this:

```
echo | ${DIR}/bin/ospatrol-logtest > /dev/null 2>&1;
```

The rules aren't on my agents, they're only on the server!

That's not a question. Also, that's the way it is. Only the server has the rules. Agents do not get a copy of the rules.

Do the rules get pushed to the agents automatically?

The rules only exist on the manager. All analysis is done on the manager. Agents do not send alerts to the manager, they only send the raw logs.

How can I get ospatrol.log to rotate daily?

Currently OSPatrol does not rotate the `ospatrol.log`, use logrotate.d or newsyslog to rotate it for now.

1.2.4 OSPatrol-WUI: FAQ

Why does the OSSE-WUI appear to be dead?

Because it is. No one has worked on it for quite a while. There may be some ongoing work with it, but as of this writing it is considered a dead project.

Why does the src ip field contain strange information instead of an IP?

Users who have installed OSPatrol-WUI 0.3, have not applied the necessary patches, and are using OSPatrol 2.6 or later may see alerts like the following:

```
2013 Feb 02 10:48:42 Rule Id: 2901 level: 3
Location: ubuntu->/var/log/dpkg.log
Src IP: 02 10:48:41 install libapr1 <none> 1.4.6-1
New dpkg (Debian Package) requested to install.
** Alert 1359830922.3553: - syslog,dpkg,
2013 Feb 02 10:48:42 ubuntu->/var/log/dpkg.log
Rule: 2901 (level 3) -> 'New dpkg (Debian Package) requested to install.'
2013-02-02 10:48:41 install libaprutil1 <none> 1.3.12+dfsg-3
```

The alert format changed in 2.6, and since OSPatrol-WUI is essentially abandonware it was not updated to handle the changes. A number of users have provided patches to correct the issues, and the OSPatrol team is planning on releasing an updated WUI containing these patches. You can find a patched version of the OSPatrol-WUI at a *bitbucket repository <https://bitbucket.org/jbcheng/ospatrol-wui>_*.

1.2.5 Syscheck: FAQ

How to force an immediate syscheck scan?

Run agent control tool to perform a integrity checking immediately (option -a to run on all the agents and -u to specify an agent id)

```
# /var/ospatrol/bin/agent_control -r -a
# /var/ospatrol/bin/agent_control -r -u <agent_id>
```

For more information see the *agent_control* documentation.

How to tell syscheck not to scan the system when OSPatrol starts?

Set the option <scan_on_start> to "no" on ospatrol.conf

How to ignore a file that changes too often?

Set the file/directory name in the <ignore> option or create a simple local rule.

The following one will ignore files /etc/a and /etc/b and the directory /etc/dir for agents mswin1 and ubuntu-dns:

```
<rule id="100345" level="0" >
    <if_group>syscheck</if_group>
    <description>Changes ignored.</description>
    <match>/etc/a|/etc/b|/etc/dir</match>
    <hostname>mswin1|ubuntu-dns</hostname>
</rule>
```

Why does OSPatrol still scan a file even though it's been ignored?

No idea. So if there are some directories you do not want scanned at all, make sure they are not included in a `<directories>` configuration.

How to know when the syscheck scan ran?

Use the agent_control tool on the manager, to see this information.

More information see the *agent_control* documentation.

How to get detailed reporting on the changes?

Use the syscheck_control tool on the manager or the web ui for that.

More information see the *syscheck_control* documentation.

Syscheck not sending any file data to the server?

With ospatrol 1.3 and Fedora you may run into this problem:

You have named files you'd like ospatrol to monitor so you add:

```
<ospatrol_config>
    <syscheck>
        <directories check_all="yes">/var/named</directories>
```

to ospatrol.conf on the client. Fedora – at least as of version 7 – runs named in a chroot jail under /var/named/chroot. However, part of that chroot jail includes /var/named/chroot/proc. The contents of that directory are purely ephemeral; there is no value to checking their integrity. And, at least in ospatrol 1.3, your syscheck may stall trying to read those files.

The symptom is a syscheck database on the server that never grows beyond a file or two per restart of the client. The log monitoring continues to work, so you know it's not a communication issue, and you will often see a slight increase in syscheck database file size after the client has restarted (in one case about 20 minutes after). But the database will never be completely built; there will only be a couple files listed in datebase.

The solution is to add an ignore clause to ospatrol.conf on the client:

```
<ospatrol_config>
    <syscheck>
        <ignore>/var/named/chroot/proc</ignore>
```

Why aren't new files creating an alert?

By default OSPatrol does not alert on new files. To enable this functionlity, <alert_new_files> must be set to yes inside the <syscheck> section of the manager's ospatrol.conf. Also, the rule to alert on new files (rule 554) is set to level 0 by default. The alert level will need to be raised in order to see the alert. Alerting on new files does not work in realtime, a full scan will be necessary to detect them.

Add the following to local_rules.xml:

```
<rule id="554" level="10" overwrite="yes">
  <category>ospatrol</category>
  <decoded_as>syscheck_new_entry</decoded_as>
  <description>File added to the system.</description>
  <group>syscheck,</group>
</rule>
```

The <alert_new_files> entry should look something like this:

```
<syscheck>
  <frequency>7200</frequency>
  <alert_new_files>yes</alert_new_files>
  <directories check_all="yes">/etc,/bin,/sbin</directories>
</syscheck>
```

Can OSPatrol include information on who changed a file in the alert?

In short, no. OSPatrol does not track this information. You could use your OS's auditing facilities to track this information, and create a rule to alert when an appropriate log is created.

1.2.6 When the unexpected happens: FAQ

How do I troubleshoot ospatrol?

If you are having problems with ospatrol, the first thing to do is to look at your logs.

- Unix/Linux: The logs will be at /var/ospatrol/logs/ospatrol.log
- Windows: The logs are at C:Program Filesospatrol-agentospatrol.log.

If by looking at them, you can't find out the error, we suggest you to send an e-mail to one of our mailing lists with the following information:

- OSPatrol version number.

  Run the following to get the version installation.

  ```
  # /var/ospatrol/bin/ospatrol-analysisd -V
  ```

- Content of /etc/ospatrol-init.conf
- Content of /var/ospatrol/etc/ospatrol.conf or (or C:Program Filesospatrol-agentospatrol.log if Windows)
- Content of /var/ospatrol/logs/ospatrol.log
- Operating system name/version (uname -a if Unix)
- Any other relevant information.

How to debug ospatrol?

> **Warning:** Only read this section if you tried to troubleshoot ospatrol already, but didn't have lucky solving your problem. Most of the users will never need to enable debugging, since it can significantly hurt performance.

Debug Logging

You can also enable debugging mode on ospatrol to extract more data about what is going on. To do so, you will need to modify the file /var/ospatrol/etc/internal_options.conf (or C:\Program Files\ospatrol-agent\internal_options.conf on Windows) and change the debug level from the default "0" to "1" or "2".

For example, if you wish to debug your windows agent, just change the option windows.debug from 0 to 2. Bellow is the list of all the debug options:

```
# Debug options.
# Debug 0 -> no debug
# Debug 1 -> first level of debug
# Debug 2 -> full debugging

# Windows debug (used by the windows agent)
windows.debug=0

# Syscheck (local, server and unix agent)
syscheck.debug=0

# Remoted (server debug)
remoted.debug=0

# Analysisd (server or local)
analysisd.debug=0

# Log collector (server, local or unix agent)
logcollector.debug=0

# Unix agentd
agent.debug=0
```

If this is on an OSPatrol server you can enable debug by running:

```
# /var/ospatrol/bin/ospatrol-control enable debug
```

Enable debug mode and restart the OSPatrol processes to view more verbose logs.

Getting more log data

If you are up to editing the source and recompiling, you can use the verbose() function to add entries to the log. This has been helpful on at least one occasion to help pinpoint where a problem was occurring. Something along these lines should work (at least in 1.3):

```
verbose("MyName: inside the_file.c the_function() %s ..", the_string);
```

- If you tag all your extra logs with something, MyName, in this example, they stand out better.
- If you need to get information from several source files, including the file name the_file.c, in this example is helpful.
- You will almost surely want information from more than one fuction, including the name, the_fuction() will show which function sent the log.

- Finally, you can include a variable string with the printf format specifier %s in the log entry and the_string is the name of the string variable to send to the log.

With some calls to verbose, recompile and replace the stock binary with your edited one. Restart ospatrol and tail the log.

The communication between my agent and the server is not working. What to do?

There are multiple reasons for it to happen. First, you should look at your agent and server logs to see what they say. If you don't know where they are, go to our Troubleshooting page for more information.

In addition to that, follow the step by step at the end, if you need to add/re-add the authentication keys.

There is a firewall between the agent and the server.

If you have the following message on the agent log:

```
2007/04/19 12:42:54 ospatrol-agentd(4101): Waiting for server reply (not started).
2007/04/19 12:43:10 ospatrol-agentd(4101): Waiting for server reply (not started).
2007/04/19 12:43:41 ospatrol-agentd(4101): Waiting for server reply (not started).
2007/04/19 12:44:27 ospatrol-agentd(4101): Waiting for server reply (not started).
```

And nothing on the server log, you probably have a firewall between the two devices. Make sure to open port 1514 UDP between them (keeping state –the agent connects to the server and expects a reply back).

Note: The way the agent/server communication works is that the agent starts a connection to the server using any random high port. So, the only port that OSPatrol opens is in the server side (port 1514 UDP). It works similar to DNS, where the DNS client connects to UDP port 53 and expects a reply back.

Wrong authentication keys configured (you imported a key from a different agent).

If that's the case, you would be getting logs similar to the above on the agent and the following on the server (see also Errors:1403):

```
2007/05/23 09:27:35 ospatrol-remoted(1403): Incorrectly formated message from 'xxx.xxx.xxx.xxx'.
2007/05/23 09:27:35 ospatrol-remoted(1403): Incorrectly formated message from 'xxx.xxx.xxx.xxx'.
```

The IP address you configured the agent is different from what the server is seeing.

Same as above (see also see Errors:1403).

Step by Step – adding the authentication keys

For most of the errors (except the firewall issue), removing and re-adding the authentication keys fix the problem. Do the following if you are having issues:

1. 'Stop the server and the agent.'
    - Make sure they are really stopped (ps on Unix or sc query ospatrolsvc on Windows)
2. Run the manage-agents tool on the server and remove the agent.
3. Still on the server, add the agent using manage-agents. Make sure the IP is correct.
4. Start the server.
5. Run manage-agents on the agent and import the newly generated key.
6. Start the agent.

If after that, it still doesn't work, contact our mailing list for help.

What does "1403 - Incorrectly formated message" means?

It means that the server (or agent) wasn't able to decrypt the message from the other side of the connection. See The communication between my agent and the server is not working. What to do?

The main reasons for this to happen are:

- Wrong authentication keys configured (you imported a key from a different agent).
- The IP address you configured the agent is different from what the server is seeing.

How to fix it:

- Check if you imported the right authentication keys into the agent.
- Check if the IP address is correctly.
- You can also try to remove the agent (using manage_agents), add it back again and re-import the keys into the agent. Make sure to restart the server (first) and then the agent after that.

What does "1210 - Queue not accessible?" mean?

Check queue/ospatrol/queue

If you have logs similar to the following in `/var/ospatrol/queue/ospatrol/queue`:

```
2008/04/29 15:40:39 ospatrol-syscheckd(1210): ERROR: Queue '/var/ospatrol/queue/ospatrol/queue' not a
2008/04/29 15:40:39 ospatrol-rootcheck(1210): ERROR: Queue '/var/ospatrol/queue/ospatrol/queue' not a
2008/04/29 15:40:45 ospatrol-logcollector(1210): ERROR: Queue '/var/ospatrol/queue/ospatrol/queue' no
2008/04/29 15:40:45 ospatrol-logcollector(1211): ERROR: Unable to access queue: '/var/ospatrol/queue/
2008/04/29 15:41:00 ospatrol-syscheckd(1210): ERROR: Queue '/var/ospatrol/queue/ospatrol/queue' not a
2008/04/29 15:41:00 ospatrol-rootcheck(1211): ERROR: Unable to access queue: '/var/ospatrol/queue/osp
```

It means that *ospatrol-analysisd* is not running for some reason.

The main reasons for this to happen are:

- *ospatrol-analysisd* didn't start properly. Look at the logs for any error from it.
- *ospatrol-analysisd* didn't start at all. There is a bug in the init scripts that during system reboot, it may not start if the PID is already in use (we are working to fix it).
- *ospatrol-analysisd* cannot access `/queue/fts/fts-queue`. Look for the error message `ospatrol-analysisd(1103): ERROR: Unable to open file '/queue/fts/fts-queue'`. This can be fixed by ensuring that the ospatrol user owns `/var/ospatrol/queue/fts/fts-queue`.

How to fix it:

Stop OSPatrol and start it back again:

```
# /var/ospatrol/bin/ospatrol-control stop
(you can also check at /var/ospatrol/var/run that there is not PID file in there)
# /var/ospatrol/bin/ospatrol-control start
```

If there is any configuration error, fix it.

Check queue/alerts/ar

If you have logs similar to the following in `/var/ospatrol/queue/alerts/ar`:

```
2009/02/17 12:03:04 ospatrol-analysisd(1210): ERROR: Queue '/queue/alerts/ar' not accessible: 'Connec
2009/02/17 12:03:04 ospatrol-analysisd(1301): ERROR: Unable to connect to active response queue.
```

It means that there is nothing listening on the other end of the socket the *ospatrol-analysisd* deamon would want to write to. This can happen in an ospatrol server installation. The deamon that should be listening on this socket is *ospatrol-remoted*.

How to fix it:

Add an OSPatrol client (agent) with the *manage_agents* utility on both agent and server. Then restart OSPatrol. *ospatrol-remoted* should now be listening on the socket.

Remote commands are not accepted from the manager. Ignoring it on the agent.conf

This error message is caused by `command` or `full_command` log types in the agent.conf. Originally OSPatrol supported running commands from the agent.conf by default. Thie was later changed as a security precaution due to the commands being run as root. When a command is encountered on an agent in the agent.conf this error will be produced and the agent may not fully start. This error may also accompany the above error message:

```
ERROR: Configuration error at '/var/ospatrol-agent/etc/shared/agent.conf'. Exiting.
```

Errors when dealing with multiple agents

When you have hundreds (or even thousands) of agents, OSPatrol may not work properly by default. There are a few changes that you will need to do:

Increase maximum number of allowed agents

To increase the number of agents, before you install (or update OSPatrol), just do:

```
#cd src; make setmaxagents (it will ask how many do you want.. )

Specify maximum number of agents: 2048 (to increase to 2048)
Maximum number of agents set to 20.

#cd ..; ./install.sh
```

Increase your system's limits

Most systems have limits regarding the maximum number of files you can have. A few commands you should try are (to increase to 2048):

```
# ulimit -n 2048
# sysctl -w kern.maxfiles=2048
```

Fixing Duplicate Errors

Ossec agents and server keep a counter of each message sent and received in files in .../ospatrol/queue/rids. This is a technique to prevent replay attacks. If the counters between agent and server don't match you'll see errors like this in the agents ospatrol.log file:

```
2007/10/24 11:19:21 ospatrol-agentd: Duplicate error:  global: 12, local: 3456, saved global: 78, sav
2007/10/24 11:19:21 ospatrol-agentd(<pid>): Duplicated counter for '<host name>'.
2007/10/24 11:19:21 ospatrol-agentd(<pid>): Problem receiving message from www.xxx.yyy.zzz.
```

This normally happens when you restore the ospatrol files from a backup or you reinstall server or agents without performing an upgrade, this can also be caused by duplicate agent ID's. The fix for this problem is:

1. On every agent:

1. stop ospatrol

2. go to: .../ospatrol/queue/rids (or ospatrol-agent/rids on Windows) and remove every file in there.

2. Go to the server:

1. Stop ospatrol

2. Remove the rids file with the same name as the agent id that is reporting errors.

3. Restart the server

4. Restart the agents.

To avoid this problem from ever happening again, make sure to:

- Always use the update option (when updating). Do not remove and reinstall the ospatrol server, unless you plan to do the same for all agents.
- Do not re-use the same agent key between multiple agents or the same agent key after you remove/re-install an agent. If you use the "update" options everything should just work.

Agent won't connect to the manager or the agent always shows never connected

The following log messages may appear in the `ospatrol.log` file on an agent when it is having issues connecting to a manager:

```
2011/11/13 18:05:13 ospatrol-agent: WARN: Process locked. Waiting for permission...
2011/11/13 18:05:24 ospatrol-agent(4101): WARN: Waiting for server reply (not started). Tried: '10.10
2011/11/13 18:05:26 ospatrol-agent: INFO: Trying to connect to server (10.10.134.241:1514).
2011/11/13 18:05:26 ospatrol-agent: INFO: Using IPv4 for: 10.10.134.241 .
2011/11/13 18:05:47 ospatrol-agent(4101): WARN: Waiting for server reply (not started). Tried: '10.10
```

If the agent's packets are making it to the manager, the manager will also include error messages in its `ospatrol.log` related to that agent. Some possible issues:

- The agent may not be using the correct IP address. Some systems with multiple IP addresses may not choose the correct one to communicate with the OSPatrol manager. Using `any` or a CIDR address (192.168.1.0/24) for the agent may be one solution, and adjusting the system's route settings is another.
- Every agent must be using a unique key. If 2 agents look like they're coming from the same IP (possibly from a NAT gateway), then `any` or the CIDR address should be used to identify them on the manager.
- There may be a firewall blocking the OSPatrol traffic, udp 1514 should be allowed to and from the manager.
- UAC may be blocking the OSPatrol service from communicating with the manager on Windows 7.

I am seeing high CPU utilization on a Windows agent

Some OSPatrol HIDS users who have deployed the Windows agent have experienced situations where the windows OSPatrol agent causes high CPU utilization. In some cases, this may be due to syscheck having to do integrity checking on a large number of files and the frequency with which this is done. The high CPU utilization could also take place when the OSPatrol agent has to analyze Windows Event logs with very large numbers of generated events.

A clue to what may be happening are alerts like these:

The above alert indicates the condition where a large number of events are being generated in the Windows event logs. In Windows, setting the Windows audit policy to Audit Object Access or Audit Process Tracking can cause the generation of many event log entries. This gives the OSPatrol agent much more work to do in log analysis, and thus

causes the consumption of much more CPU cycles. To reduce the CPU utilization in this case, the solution is to disable auditing of object access and/or process tracking. Typically, these audit settings aren't required except for debugging purposes, or situations in which you absolutely have to track everything.

CHAPTER 2

Reference

2.1 Syntax and Options

2.1.1 Regular Expression Syntax

Currently OSPatrol supports to regex syntax:

- OS_Regex or regex
- OS_Match or sregex

OR_Regex/regex Syntax

Fast and simple library for regular expressions in C.

This library is designed to be simple, but support the most common regular expressions. It was designed with intrusion detection systems in mind, where having all options is not crucial, but speed is. **Supported expressions**:

```
\w  ->  A-Z, a-z, 0-9 characters
\d  ->  0-9 characters
\s  ->  For spaces " "
\t  ->  For tabs.
\p  ->  ()*+,-.:;<=>?[] (punctuation characters)
\W  ->  For anything not \w
\D  ->  For anything not \d
\S  ->  For anything not \s
\.  ->  For anything
```

Modifiers:

```
+  ->  To match one or more times (eg \w+ or \d+)
*  ->  To match zero or more times (eg \w* or \p*)
```

Special Characters:

```
^ -> To specify the beginning of the text.
$ -> To specify the end of the text.
| -> To create an "OR" between multiple patterns.
```

Characters Escaping

To utilize the following characters they must be escaped:

```
$ -> \$
( -> \(
) -> \)
\ -> \\
| -> \|
```

OS_Match/sregex Syntax

Faster than the OS_Regex/regex, but only supports simple string matching and the following special characters.

Special Characters:

```
^ -> To specify the beginning of the text.
$ -> To specify the end of the text.
| -> To create an "OR" between multiple patterns.
```

2.1.2 Log Analysis Syntax: Rules and Decoders

Rules Syntax

Overview

Options

rule
Defines a rule

Attributes:

- *level*
  - Specifies the level of the rule. Alerts and responses use this value.
  - **Allowed:** Any number (0 to 16)
- *id*
  - Specifies the ID of the rule.
  - **Allowed:** Any number from 100 to 99999
- *maxsize*
  - Specifies the maximum size of the event.
  - **Allowed:** Any number from 1 to 99999
- *frequency*
  - Specifies the number of times the rule must have matched before firing. The number that triggers the rule is actually 2 more than this setting.
  - **Allowed:** Any number from 1 to 999

–**Example:** frequency="2" would mean the rule must be matched 4 times

Note: More information about how frequency is counted can be found in this thread.

•*timeframe*

–The timeframe in seconds.

–This option is intended to be used with the frequency option.

–**Allowed:** Any number from 1 to 9999

•*ignore*

–The time (in seconds) to ignore this rule after firing it (to avoid floods).

–**Allowed:** Any number from 1 to 9999

•***overwrite***

– Used to supercede an OSPatrol rule with local changes.

– This is useful to change the level or other options of rules included with OSPatrol.

– **Allowed** yes

match

•Any string to match against the log event.

•**Allowed:** Any *OS_Match/sregex Syntax*

regex

•Any regex to match against the log event.

•**Allowed:** Any *OR_Regex/regex Syntax*

decoded_as

•Any decoder name (see *Decoders Syntax*)

•**Allowed:** Any decoder name

category

•The decoded category to match (ids, syslog, firewall, web-log, squid or windows).

•**Allowed:** Any category *categories*

srcip

•Any IP address or CIDR block to be compared to an IP decoded as srcip.

•Use "!" to negate it.

•**Allowed:** Any srcip

dstip

•Any IP address or CIDR block to be compared to an IP decoded as dstip.

•Use "!" to negate it.

•**Allowed:** Any dstip

user

- Any username (decoded as the username).
- **Allowed:** any *OS_Match/sregex Syntax*

program_name

- Program name is decoded from syslog process name.
- **Allowed:** any *OS_Match/sregex Syntax*

hostname

- Any hostname (decoded as the syslog hostname) or log file.
- **Allowed:** any *OS_Match/sregex Syntax*

time

- Time that the event was generated.
- **Allowed:** Any time range (hh:mm-hh:mm)
- **Example:** `<time>6 am - 6 pm</time>`

weekday

- Week day that the event was generated.
- **Allowed:** monday - sunday, weekday, weekend

id

- Any ID (decoded as the ID).
- **Allowed:** any *OS_Match/sregex Syntax*

url

- Any URL (decoded as the URL).
- **Allowed:** any *OS_Match/sregex Syntax*

if_sid

- Matches if the ID has matched.
- **Allowed:** Any rule id

if_group

- Matches if the group has matched before.
- **Allowed:** Any Group

if_level

- Matches if the level has matched before.
- **Allowed:** Any level from 1 to 16

if_matched_sid

- Matches if an alert of the defined ID has been triggered in a set number of seconds.
- This option is used in conjunction with frequency and timeframe.

Note: Rules at level 0 are discarded immediately and will not be used with the `if_matched_` rules. The level must be at least `1`, but the `<no_log>` option can be added to the rule to make sure it does not get logged.

- **Allowed:** Any rule id

if_matched_group

- Matches if an alert of the defined group has been triggered in a set number of seconds.
- This option is used in conjunction with frequency and timeframe.
- **Allowed:** Any group

if_matched_level

- Matches if an alert of the defined level has been triggered in a set number of seconds.
- This option is used in conjunction with frequency and timeframe.
- **Allowed:** Any level from 1 to 16

same_source_ip

- Specifies that the source ip must be the same.
- This option is used in conjunction with frequency and timeframe.

Example: <same_source_ip />

same_source_port

- Specifies that the source port must be the same.
- This option is used in conjunction with frequency and timeframe.
- **Example:** <same_source_port />

same_dst_port

- Specifies that the destination port must be the same.
- This option is used in conjunction with frequency and timeframe.
- **Example:** <same_source_port />

same_location

- Specifies that the location must be the same.
- This option is used in conjunction with frequency and timeframe.
- **Example:** <same_location />

description

- Rule description.
- **Allowed:** Any string

list

Preform a CDB lookup using an OSPatrol list. This is a fast on disk database which will always find keys within two seeks of the file.

Attributes:

- *field*

  Field that is used as the key to look up in the CDB file:

  – Value: srcip

  – Value: srcport

- Value: dstip
- Value: dstport
- Value: user
- Value: url
- Value: id
- Value: hostname
- Value: program_name
- Value: status
- Value: action

- *lookup*

  This is the type of lookup that is preformed:

  - Value: match_key
    - Positive key match: field is the key to search within the cdb and will match if they key is present.
    - This is the default if no lookup is specified.
  - Value: not_match_key
    - Negative key match: field is the key to search and will match if it *IS NOT* present in the database.
  - Value: match_key_value
    - Key and Value Match: field is searched for in the cdb and if found the value will be compared with regex from attribute check_value.

    Note: This feature is not yet complete.
  - Value: address_match_key
    - Positive key match: field is an IP address and the key to search within the cdb and will match if they key is present.
  - Value: not_address_match_key
    - Negative key match: field is an IP address the key to search and will match if it *IS NOT* present in the database.
  - Value: address_match_key_value
    - Key and Value Match: field is an IP address searched for in the cdb and if found the value will be compared with regex from attribute check_value.

    Note: This feature is not yet complete.

- *check_value*
  - regex pattern for matching on the value pulled out of the cdb when using lookup types: address_match_key_value, match_key_value

Allowed:

Path to the CDB file to be used for lookup from the OSPatrol directory. This file must also be included in the ospatrol.conf file.

Example:

```
<rule id="100000" level="7">
  <list lookup="match_key" field="srcip">path/to/list/file</list>
  <description>Checking srcip against cdb list file</description>
</rule>
```

info

Extra information may be added through the following attributes:

Attributes:

- *type*
  - Value: text

    This is the default when no type is selected. Just used for additional information about the alert/event.

  - Value: link

    Link to more information about the alert/event.

  - Value: cve

    The CVE Number related to this alert/event.

  - Value: ovsdb

    The osvdb id related to this alert/event.

Allowed: String but content is dependent on the type attribute.

Example:

```
<rule id="502" level="3">
    <if_sid>500</if_sid>
    <options>alert_by_email</options>
    <match>OSPatrol started</match>
    <description>OSPatrol server started.</description>
    <info type="link">http://ospatrol.com/go/rule:205</info>
    <info type="cve">2009-1002</info>
    <info type="osvdb"> 61509</info>
    <info type="text">Internal Why we are running this run in our company</info>
    <info>Type text is the default</info>
</rule>
```

options

Additional rule options

Allowed:

- ***alert_by_email***
  - Always alert by email.
  - *Example:* <options>alert_by_email</options>
- ***no_email_alert***
  - Never alert by email.
  - *Example:* <options>no_email_alert</options>

- **no_log**
  - Do not log this alert.
  - *Example:* <options>no_log</options>

check_diff
Used to determine when the output of a command changes.

Usage: <check_diff />

Additional info: Daniel Cid has written a blog post about the feature.

group

- Add additional groups to the alert. Groups are optional tags added to alerts. They can be used by other rules by using `if_group` or `if_matched_group`, or by alert parsing tools to categorize alerts.

  Example: <group>group1, group2</group>

Decoders Syntax

Overview

Options

decoder
Attributes:

- *id:*:
- *name*:
- *type*:
- *status*:

decoder.parent

decoder.program_name
Allowed: Any *OS_Match/sregex Syntax*

decoder.prematch
Allowed: Any *OS_Match/sregex Syntax*

decoder.regex
Allowed: Any *OR_Regex/regex Syntax*

decoder.order
Allowed:

- location - where the log came from (only on FTS)
- srcuser - extracts the source username
- dstuser - extracts the destination (target) username
- user - an alias to dstuser (only one of the two can be used)
- srcip - source ip
- dstip - dst ip
- srcport - source port

- dstport - destination port
- protocol - protocol
- id - event id
- url - url of the event
- action - event action (deny, drop, accept, etc)
- status - event status (success, failure, etc)
- extra_data - Any extra data

decoder.fts

decoder.ftscomment
Unused at this time.

2.1.3 ospatrol.conf: syntax and options

ospatrol.conf: Active Response Options

Overview

Supported types Active-reponse options are available in the the following installation types:

- server
- local

Configuration pieces There are two pieces to an active-response configuration. The first is the `<command>` section. This details the command to be run, and the options it will use. There can be any number of command options.

The second is the `<active-response>` section. This section defines when the command will be run.

Location All active-response options must be configured in the /var/ospatrol/etc/ospatrol.conf and used within the <ospatrol_config> tag.

XML excerpt to show location:

```
<ospatrol_config>
    <command>
        <!--
        Command options here
        -->
    </command>
    <active-response>
        <!--
        active-response options here
        -->
    </active-response>
</ospatrol_config>
```

Command Options

command
In the commands configuration you create new "commands" to be used as responses. You can have as many commands as you want. Each one should be inside their own "command" element. `command` is required.

name
Used to link the command to the response. `name` is required.

executable
It must be a file (with exec permissions) inside `/var/ospatrol/active-response/bin`. `executable` is required.

You don't need to provide the whole path.

expect
The arguments this command is expecting (options are srcip and username). If a field is not within the `expect` option it will be passed as a dash (-) instead of the actual value. For instance, if `srcip` is required for an active-response script to work it **must** be inside of an `expect` option. `expect` is required.

Note: `expect` is required, but it is not reqiured to populate it. `<expect></expect>` is valid if no options need to be passed to the active-response script.

---

timeout_allowed
Specifies if this command supports a timeout. This is optional, and defaults to `yes`.

Active-response Options

active-response
In the active-response configuration, you bind the commands (created) to events. You can have as many responses as you want. Each one should be inside their own "active-response" element.

disabled
Disables active response if set to yes. If this is not defined active response is enabled.

command
Used to link the response to the command

location
Where the command should be executed. You have four options:

Allowed:

- *local*: on the agent that generated the event
- *server*: on the OSPatrol server
- *defined-agent*: on a specific agent (when using this option, you need to set the agent_id to use)
- *all*: or everywhere.

agent_id
The ID of the agent to execute the response (when defined-agent is set).

level
The response will be executed on any event with this level or higher.

rules_group
The response will be executed on any event in the defined group. Multiple groups can be defined if separated by a comma.

rules_id
The response will be executes on any event with the defined ID. Multiple IDs can be specified if separated by a comma.

timeout
How long in seconds until the reverse command is executed (IP unblocked, for example).

repeated_offenders
A comma separated list of increasing timeouts in minutes for repeat offenders. There can be a maximum of 5 entries. This should be set in the `ospatrol.conf` of an agent in an agent/server setup.

Example:

```
<active-response>
  <command>firewall-block</command>
  <location>defined-agent</location>
  <agent_id>001</agent_id>
  <rules_group>authentication_failed,authentication_failures</rules_group>
  <timeout>600</timeout>
  <repeated_offenders>30,60,120</repeated_offenders>
</active-response>

<active-response>
  <repeated_offenders>30,60,120</repeated_offenders>
</active-response>
```

Example active response configurations:

Command: Restart OSPatrol on *nix systems: This command can be used to restart the OSPatrol processes. It's commonly used to automatically restart agent processes when an `agent.conf` is modified. Since no parameters are necessary the `<expect>` is empty.

```
<command>
  <name>restart-ospatrol</name>
  <executable>restart-ospatrol.sh</executable>
  <expect></expect>
</command>
```

Active-Response: Restart the OSPatrol processes: This active response will restart the OSPatrol processes using the `restart-ospatrol` command above. It is runs when rule `510010` is triggered, and it runs on the system where the rule was triggered.

```
<active-response>
  <command>restart-ospatrol</command>
  <location>local</location>
  <rules_id>510010</rules_id>
</active-response>
```

Here is an example rule checking for changes to the `agent.conf`.

```
<rule id="510011" level="10">
  <if_sid>550</if_sid>
  <match>/var/ospatrol/etc/shared/agent.conf</match>
  <description>agent.conf has been modified</description>
</rule>
```

Command: Block an IP with pf.sh: `pf.sh` adds an ip (`srcip`) to an `ospatrol_fwtable` packet filter table. Information on pf tables can be found here.

```
<command>
  <name>pf-block</name>
  <executable>pf.sh</executable>
  <expect>srcip</expect>
</command>
```

This is the minimum configuration necessary to utilize `pf.sh`:

```
table <ospatrol_fwtable> persist #ospatrol_fwtable
block in log quick from <ospatrol_fwtable>
```

Active-Response: Block an IP with pf: This active-response blocks an IP triggering an `authentication_failed` or `authentication_failures` alert. This active-response will run on agent `001` only.

```
<active-response>
  <command>pf-block</command>
  <location>defined-agent</location>
  <agent_id>001</agent_id>
  <rules_group>authentication_failed,authentication_failures</rules_group>
</active-response>
```

Command: Run the makelists.sh script: The `makelists.sh` script runs `/var/ospatrol/bin/ospatrol-makelists` to update cdb lists. This command can be triggered by changes in configured cdb lists.

```
<command>
  <name>makelists</name>
  <executable>makelists.sh</executable>
  <expect>hostname</expect>
</command>
```

Active-Response: Update cdb lists: This active-response will run the `makelists` command to update the cdb lists. This active-response should run only on the OSPatrol server since agents do not have cdb lists.

```
<active-response>
  <command>makelists</command>
  <location>server</location>
  <rules_id>510011</rules_id>
</active-response>
```

Rule 510011: This example rule looks for changes to `/var/ospatrol/lists/blocked.txt` based on syscheck alerts.

```
<rule id="510011" level="10">
  <if_sid>550</if_sid>
  <match>/var/ospatrol/lists/blocked.txt</match>
  <description>blocked.txt has been modified</description>
</rule>
```

Command: firewall-drop: This is a command to run the `firewall-drop.sh` script to block the `srcip`.

```
<command>
  <name>firewall-drop</command>
  <executable>firewall-drop.sh</executable>
  <expect>srcip</expect>
</command>
```

Active-Response: Block a srcip: This active-response will use the `firewall-drop` command to block an IP address that has triggered an `authentication_failed` or `authentication_failures` alert. It will run on all agents, and has a timeout of 600 seconds. It also uses the `repeated_offenders` option blocking an IP for 30 minutes on the second infraction, 60 minutes on the third, etc.

```
<active-response>
  <command>firewall-block</command>
  <location>all</location>
  <rules_group>authentication_failed,authentication_failures</rules_group>
  <timeout>600</timeout>
  <repeated_offenders>30,60,120</repeated_offenders>
</active-response>
```

ospatrol.conf: Agentless Options

Overview

Supported types Agentless options are available in the the following installation types:

- server
- local

Location All agentless options must be configured in the /var/ospatrol/etc/ospatrol.conf and used within the <ospatrol_config> tag.

XML excerpt to show location:

```
<ospatrol_config>
    <agentless>
        <!--
        agentless options here
        -->
    </agentless>
</ospatrol_config>
```

Options

agentless
: This is the section that will contain the agentless configuration.

frequency
: This controls the number of seconds between each run.

host
: This defines the username and agentless host.

  Example:

```
<host>root@linux.server.example.com</host>
```

state
This determines whether the checks are periodic or periodic_diff.

- periodic: The output from the scripts is processed by the OSPatrol processes.
- periodic_diff: The output from the scripts is compared to the output of previous runs.

arguments
This defines the arguments passed to the script.

ospatrol.conf: Alerts Options

Overview

Supported types Alerts options are available in the the following installation types:

- server
- local

Location All alerts options must be configured in the /var/ospatrol/etc/ospatrol.conf and used within the <ospatrol_config> tag.

XML excerpt to show location:

```
<ospatrol_config>
    <alerts>
        <!--
        alerts options here
        -->
    </alerts>
</ospatrol_config>
```

Options

alerts

email_alert_level
Minimum alert level to send e-mail notifications.

Default: 7

Allowed: Any level from 1 to 16

Note: This is the minumum level for an alert to trigger an email. This overrides granular email alert levels. Setting this to 10 would prevent emails for alerts at levels lower than 10 to be sent despite settings in the granular email configuration. Individual rules can override this with the alert_by_email option.

---

log_alert_level
Minimum alert level to store the log messages.

Default: 1

Allowed: Any level from 1 to 16

use_geoip
Enable or disable GeoIP lookups.

Default: Disabled

Allowed: yes/no

ospatrol.conf: Client Options

Overview

Supported types client options are available in the the following installation types:

- agent

Location All client options must be configured in the /var/ospatrol/etc/ospatrol.conf and used within the <ospatrol_config> tag.

XML excerpt to show location:

```
<ospatrol_config>
    <client>
        <!--
        client options here
        -->
    </client>
</ospatrol_config>
```

Options

server-ip
Specify the IP address of the analysis server

Allowed: Any Valid IP Address

server-hostname
Specify the hostname of the analysis server

Allowed: Any Valid hostname

port
Specifies the port to send the events (must be the same to the one used by the analysis server).

Default: 1514

Allowed: Any port number from 1 to 65535

server-ip
Specifies the `agent.conf` profiles to be used by the agent.

notify_time
Specifies the time in seconds between information messages sent by the agents to the server.

ospatrol.conf: Database Output options

Overview

Supported types Database Output options are available in the the following installation types:

- server
- local

Location All database_output options must be configured in the /var/ospatrol/etc/ospatrol.conf and used within the <ospatrol_config> tag.

XML excerpt to show location:

```
<ospatrol_config>
    <database_output>
        <!--
        Database Output options here
        -->
    </database_output>
</ospatrol_config>
```

Options

database_output

hostname
IP Address of the database server.

Allowed: any valid IP address

username
Username to access the database.

Allowed: Any Valid Username

password
Password to access the database.

Allowed: Any Password

database
Database name to store the alerts.

Allowed: database name

type
Type of database (Mysql or PostgreSQL).

Note: OSPatrol must be compiled with the database type that is to be used.

Allowed: mysql/postgresql

ospatrol.conf: Granular Email options

Overview

Supported types Global options are available in the the following installation types:

- server
- local

Notes Global email configuration is necessary to use the granular email options.

Location All global options must be configured in the /var/ospatrol/etc/ospatrol.conf and used within the <ospatrol_config> tag.

XML excerpt to show location:

```
<ospatrol_config>
    <email_alerts>
        <!--
        Email_alerts options here
        -->
    </email_alerts>
</ospatrol_config>
```

Options

email_alerts

email_to
E-Mail recipients of alerts

Allowed: Any valid e-mail address

level
Minimum alerting level to forward the e-mails.

Allowed: Any alert level 0 to 16

Note: `level` should be set at or above the email_alert_level in the `<alerts>` section of the configuration.

---

group
The alert that must match this group to be forwarded.

Allowed: One group or category

event_location
The alert must match this event location to be forwarded. If multiple `<event_location>` options are specified, the last will be used.

Allowed: Any single agent name, hostname, ip address, or log file

format
Specifies the format of the e-mail

- full: for normal e-mails
- sms: for reduced size suitable for SMS

Default: full

Allowed: full/sms

rule_id
Option to send granular emails based on rule id.

Allowed: * One or more rule IDs can be used here, separated by a comma and space (“, “).

Example:

```
<rule_id>5701, 5702</rule_id>
```

do_not_delay
Option to send the e-mail right away (no delay).

Example:

```
<do_not_delay />
```

do_not_group
Option to do not group alerts for this e-mail.

Example:

```
<do_not_group />
```

Examples

Example email alerts configurations:

Global Configuration:

```
<global>
  <email_notification>yes</email_notification>
  <email_to>admin@example.com</email_to>
  <smtp_server>127.0.0.1</smtp_server>
  <email_from>ospatrolm@example.com</email_from>
</global>
```

Global Configuration with a larger maximum emails per hour:

```
<global>
  <email_notification>yes</email_notification>
  <email_to>admin@example.com</email_to>
  <smtp_server>127.0.0.1</smtp_server>
  <email_from>ospatrolm@example.com</email_from>
  <email_maxperhour>100</email_maxperhour>
</global>
```

Granular Email alert: Level 12 and above:

```
<email_alerts>
  <email_to>other_admin@example.com</email_to>
  <level>12</level>
</email_alerts>
```

Syscheck alerts to syscheck admin address:

```
<email_alerts>
  <email_to>syscheck-admin@example.com</email_to>
  <group>syscheck</group>
</email_alerts>
```

Level 15 alerts from agent007 without delay or grouping:

```
<email_alerts>
  <email_to>bond@example.com</email_to>
  <event_location>agent007</event_location>
  <level>15</level>
  <do_not_delay />
  <do_not_group />
</email_alerts>
```

ospatrol.conf: Global options

Overview

Supported types Global options are available in the the following installation types:

- server
- local

Location All global options must be configured in the /var/ospatrol/etc/ospatrol.conf and used within the <ospatrol_config> tag.

XML excerpt to show location:

```
<ospatrol_config>
    <global>
        <!--
        Global options here
        -->
    </global>
</ospatrol_config>
```

Options

global

email_notification
Enable or disable e-mail alerting.

Default: no

Allowed: yes/no

email_to
E-mail recipient of the alerts.

Allowed: Any valid e-mail address

Note: To use granular email configurations, a base configuration is necessary in the `<global>` section.

email_from
E-mail "source" of the alerts.

Allowed: Any valid e-mail address

smtp_server
SMTP server.

Allowed: Any valid hostname or IP Address

email_maxperhour
Specifies the maximum number of e-mails to be sent per hour. All emails in excess of this setting will be queued for later distribution.

Default: 12

Allowed: Any number from 1 to 9999

Note: At the end of the hour any queued emails will be sent together in one email. This is true whether the mail grouping is enabled or disabled.

---

custom_alert_output
Specifies the format of alerts written to the logfile.

```
Variables:
"$TIMESTAMP"    -       The time the event was processed by OSPatrol.
"$FTELL"        -       Unknown
"$RULEALERT"    -       Unknown
"$HOSTNAME"     -       Hostname of the system generating the event.
"$LOCATION"     -       The file the log messages was saved to.
"$RULEID"       -       The rule id of the alert.
"$RULELEVEL"    -       The rule level of the alert.
"$RULECOMMENT"  -       Unknown
"$SRCIP"        -       The source IP specified in the log message.
"$DSTUSER"      -       The destination user specified in the log message.
"$FULLLOG"      -       The original log message.
"$RULEGROUP"    -       The groups containing the rule.
```

stats
Alerting level for the events generated by the statistical analysis.

Default: 8

Allowed: Any level from 0 to 16

logall
States if we should store all the events received.

Default: no

Allowed: yes/no

memory_size
Sets the memory size for the event correlation.

Default: 1024

Allowed: Any size from 16 to 5096

white_list
List of IP addresses that should never be blocked by the active response (one per element). This option is only valid in server and local installs.

Multiples Allowed: yes

Allowed: Any IP address or netblock

host_infomation
Alerting level for the events generated by the host change monitor.

Default: 8

Allowed: Any level from 0 to 16

prelude_output
Enables or disables prelude output.

Default: no

Allowed: yes/no

picviz_output
Enable picviz output.

> **Warning:** PicViz is experimental.

Allowed: yes

picviz_socket
The full path of the socket that ospatrol will write alerts/events to. This will then be read by picviz for processing.

Allowed: File and path that ospatrol will create and feed events to.

geoip_db_path
The full path to the GeoIP IPv4 database file location.

Example:

```
<geoip_db_path>/etc/GeoLiteCity.dat</geoip_db_path>
```

ospatrol.conf: Localfile options

Overview

Supported types Localfile options are available in the the following installation types:

- server
- local

Location All localfile options must be configured in the /var/ospatrol/etc/ospatrol.conf or /var/ospatrol/etc/shared/agent.conf and used within the <ospatrol_config> or <agent_config> tags.

XML excerpt to show location:

```
<ospatrol_config>
    <localfile>
        <!--
        Localfile options here
        -->
    </localfile>
</ospatrol_config>
```

Options

localfile

location

Specify the location of the log to be read. strftime formats may be used for log file names. For instance, a log file named `file.log-2011-01-22` could be referenced with `file.log-%Y-%m-%d`. Wildcards may be used on non-Windows systems. When wildcards are used, the log files must exist at the time `ospatrol-logcollector` is started. It will not automatically begin monitoring new log files. `strftime` and wildcards cannot be used on the same entry.

Default: Multiple (eg /var/log/messages)

Allowed: Any log file

log_format

The format of the log being read.

Note: If the log has one entry per line, use syslog.

Default: syslog

Allowed:

- **syslog** This format is for plain text files in a syslog-like format. It can also be used when there is no support for the logging format, and the logs are single line messages.
- **snort-full** This is used for Snort's full output format.
- **snort-fast** This is used for Snort's fast output format.
- squid
- iis
- **eventlog** This is used for Microsoft Windows eventlog format.
- **mysql_log** This is used for MySQL logs. It does not support multi-line logs.
- **postgresql_log** This is used for PostgreSQL logs. It does not support multi-line logs.
- **nmapg** This is used for monitoring files conforming to the grepable output from nmap.
- **apache**

  This format is for apache's default log format.

  Example:

- **command** This format will be the output from the command (as run by root) defined by command. Each line of output will be treated as a separate log.
- **full_command** This format will be the output from the commandi (as run by root) defined by command. The entire output will be treated as a single log.

Warning: `command` and `full_command` cannot be used in the agent.conf, and must be configured in each system's ospatrol.conf.

•djb-multilog

•**multi-line** This option will allow applications that log multiple lines per event to be monitored. This format requires the number of lines to be consistent. `multi-line:` is followed by the number of lines in each log entry. Each line will be combined with the previous lines until all lines are gathered. There may be multiple timestamps in a finalized event.

Allowed: <log_format>multi-line: NUMBER</log_format>

Example: Log messages:

```
Aug  9 14:22:47 hostname log line one
Aug  9 14:22:47 hostname log line two
Aug  9 14:22:47 hostname log line three
Aug  9 14:22:47 hostname log line four
Aug  9 14:22:47 hostname log line five
```

Log message as analyzed by **ospatrol-analysisd_**:

```
Aug  9 14:22:47 hostname log line one Aug  9 14:22:47 hostname log line two Aug  9
```

command

The command to be run. All output from this command will be read as one or more log messages depending on whether command or full_command is used.

Allowed: Any commandline and arguments.

alias

An alias to identify the command. This will replace the command in the log message.

For example `<alias>usb-check</alias>` would replace:

```
ospatrol: output: 'reg QUERY HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR':
```

with:

```
ospatrol: output: 'usb-check':
```

Allowed: Any string.

frequency

The minimum time in seconds between command runs. The command will probably not run every `frequency` seconds exactly, but the time between runs will not be shorter than this setting. This is used with command and full_command.

Allowed: Time in seconds.

check_diff

The output from an event will be stored in an internal database. Every time the same event is received, the output is compared to the previous output. If the output has changed an alert will be generated.

ospatrol.conf: Remote Options

Overview

Supported types remote options are available in the the following installation types:

- server

Location All remote options must be configured in the /var/ospatrol/etc/ospatrol.conf and used within the <ospatrol_config> tag.

XML excerpt to show location:

```
<ospatrol_config>
    <remote>
        <!--
        remote options here
        -->
    </remote>
</ospatrol_config>
```

Options

remote

connection
Specify the type of connection being enabled: secure or using syslog.

Default: secure

Allowed: secure/syslog

port
Specifies the port to listen for events.

Default:

- 1514: if connection is set to *secure*
- 514: if connection is set to *syslog*

Allowed: Any port number from 1 to 65535

protocol
Specifies the protocol to use for syslog events.

Default: udp

Allowed: udp or tcp

allowed-ips
List of IP addresses that are allowed to send syslog messages to the server (one per element).

Allowed: Any IP address or network

Note: It is necessary to allow at least one IP address when using the syslog connection type.

---

deny-ips
List of IP addresses that are not allowed to send syslog messages to the server(one per element).

Allowed: Any IP address or network

local_ip
Local ip address to listen for connections.

Default: all interfaces

Allowed: Any internal ip address

ipv6
Local ipv6 address to listen for connections.

Default: None

Allowed: Any IPv6 address.

Note: This is not well tested. For the time being I recommend using the full IPv6 address instead of one of the many shortcuts.

---

ospatrol.conf: Reports options

Overview

Supported types Reports options are available in the the following installation types:

- server
- local

Location All reports options must be configured in the /var/ospatrol/etc/ospatrol.conf and used within the <ospatrol_config> tag.

XML excerpt to show location:

```
<ospatrol_config>
    <reports>
        <!--
        Reports options here
        -->
    </reports>
</ospatrol_config>
```

Options

reports

group
Filter by group/category.

Allowed: Any category used within OSPatrol Rules.

categories
Filter by group/category.

Note: This is the same as the group option above.

Allowed: Any category used within OSPatrol Rules.

rule
Rule ID to Filter for.

Allowed: Any Rule ID in OSPatrol Rules.

level
Alert level to filter for. This is an inclusive option so all higher level alerts will also match.

Allowed: Any Alert level 1 to 16

location
Filter by the log location or agent name.

Allowed: Any file path or hostname or network.

srcip
Filter by the source ip of the event.

Allowed: Any hostname or network

user
Filter by the user name. This will match on either srcuser or dstuser

Allowed: Any username

title
The name of the report.

This is a required field for reports to function.

Allowed: Any Text

email_to
The email address to send the completed report.

This is a required field for a report to function.

Allowed: Any email address

showlogs
Include logs when creating the report

Allowed: yes/no

Default: no

ospatrol.conf: Rootcheck options

Overview

Supported types rootcheck options are available in the the following installation types:

- server
- local
- agent

Location All rootcheck options must be configured in the /var/ospatrol/etc/ospatrol.conf or /var/ospatrol/etc/shared/agents.conf and used within the <ospatrol_config> tag.

XML excerpt to show location if part of ospatrol.conf:

```
<ospatrol_config>
    <rootcheck>
        <!--
        rootcheck options here
        -->
    </rootcheck>
</ospatrol_config>
```

XML excerpt to the Location if part of agent.conf

```
<agent_config>
    <rootcheck>
        <!--
        rootcheck options here
        -->
    </rootcheck>
</agent_config>
```

Options

base_directory
The base directory that will be appended to the following options:

- rootkit_files
- rootkit_trojans
- windows_malware
- windows_audit
- windows_apps
- systems_audit

Allowed: Path to a directory **Default:** /var/ospatrol

rootkit_files
This option can be used to change the location of the rootkit files database.

Allowed: A file with the rootkit files signatures

Default: /etc/shared/rootkit_files.txt

rootkit_trojans
This option can be used to change the location of the rootkit trojans database.

Default: /etc/shared/rootkit_trojans.txt

Allowed: A file with the trojans signatures

windows_audit

system_audit

windows_apps

windows_malware

scanall
Tells rootcheck to scan the whole system (may lead to some false positives).

Default: no

Allowed: yes/no

frequency
Frequency that the rootcheck is going to be executed (in seconds).

Defaults: 36000 (10 hours)

Allowed: Time (in seconds)

disabled
Disables the execution of rootcheck.

Default: no

Allowed: yes/no

check_dev
Enable or disable the checking of something

Default: yes

Allowed: yes or no

check_files
Enable or disable the checking of something

Default: yes

Allowed: yes or no

check_if
Enable or disable the checking of something

Default: yes

Allowed: yes or no

check_pids
Enable or disable the checking of something

Default: yes

Allowed: yes or no

check_policy
Enable or disable the checking of something

Default: yes

Allowed: yes or no

check_ports
Enable or disable the checking of network ports.

Default: yes

Allowed: yes or no

check_sys
Enable or disable the checking of something

Default: yes

Allowed: yes or no

check_trojans
Enable or disable the checking of trojans.

Default: yes

Allowed: yes or no

check_unixaudit
Enable or disable the checking of something

Default: yes

Allowed: yes or no

check_winapps
Enable or disable the checking of something

Default: yes

Allowed: yes or no

check_winaudit
Enable or disable the checking of something

Default: 1

Allowed: 1 or 0

check_winmalware
Enable or disable the checking of Windows malware.

Default: yes

Allowed: yes or no

ospatrol.conf: Rules options

Overview

Supported types Rules options are available in the the following installation types:

- server
- local

Location All global options must be configured in the /var/ospatrol/etc/ospatrol.conf and used within the <ospatrol_config> tag.

XML excerpt to show location:

```
<ospatrol_config>
    <rules>
        <!--
        Rules options here
        -->
    </rules>
</ospatrol_config>
```

Options

include
Load a single rule file.

Allowed: Path and file name of rule to load example: rules/config.xml

rule

Load a single rule file.

Allowed: Path and file name of rule to load example: rules/config.xml

Note: This is the same as include, but created to keep the syntax constant with other sections of the rules config.

rule_dir

Load a directory of rules. The order of loaded files will be in alphebical order and will not load any files that have been loaded before.

Attributes:

- *pattern*: is a regex match string use to determine if a file needs to be loaded.
  - *Defaults*: regex "_rules.xml$" is used unless another one is specified.

Allowed: Path to a directory of rule files

Example:

1.Loading all rules in directory /var/ospatrol/rules ending ending with _rules.xml

```
<ospatrol_config>
    <rules>
        <rule_dir>rules</rule_dir>
    </rules>
</ospatrol_config>
```

2.Loading all rules in directory /var/ospatrol/rules/plugins ending with .xml

```
<ospatrol_config>
    <rules>
        <rule_dir pattern=".xml$">rules</rule_dir>
    </rules>
</ospatrol_config>
```

decoder

Load a single decoder file. The path should be relative to the install directory, typically `/var/ospatrol`.

Note: If no decoders are specified in ospatrol.conf the legacy `etc/decoder.xml` and `etc/local_decoder.xml` are loaded

Warning: If `<decoder>` or `<decoder_dir>` are used, the default decoder.xml will not be used. It must be specified explicitly.

Allowed: Path and file name of decoder to load example: rules/decoder/decoder.xml

decoder_dir

Load a directory of decoders. The order of loaded files will be in alphebics order and will not load any files that have been loaded before. The path should be relative to the install directory, typically `/var/ospatrol`.

Attributes:

- *pattern*: is a regex match string use to detemine if a file needs to be loaded.
  - *Defaults*: regex "_decoder.xml$" is used unless another one is specified.

Allowed: Path to a directoy of decoder files

Example:

1.Loading all decoders in directory /var/ospatrol/rules ending ending with _decoder.xml

```
<ospatrol_config>
    <rules>
        <decoder_dir>rules</decoder_dir>
    </rules>
</ospatrol_config>
```

2.Loading all decoders in directory /var/ospatrol/rules/plugins/plugins/decoders ending with .xml

```
<ospatrol_config>
    <rules>
        <decoder_dir pattern=".xml$">rules/plugins/decoders</decoder_dir>
    </rules>
</ospatrol_config>
```

Warning: If <decoder> or <decoder_dir> are used, the default decoder.xml will not be used. It must be specified explicitly.

list

Load a single cdb references for inclusion by other rules.

Note: Due to the way cdb files are compiled using tmp files by the *ospatrol-makelists* program the file extension should not be include in this directive. ospatrol's tools will correctly append the correct .cdb or .txt extension as needed.

Allowed: Path to a list file to be loaded and compiled.

ospatrol.conf: Syscheck Options

Overview

Supported types Syscheck options are available in the the following installation types:

- server
- local
- agent

Location All global options must be configured in the /var/ospatrol/etc/ospatrol.conf and used within the <ospatrol_config> tag.

XML excerpt to show location:

```
<ospatrol_config>
    <syscheck>
        <!--
        Syscheck options here
        -->
    </syscheck>
</ospatrol_config>
```

Options

directories

Use this option to add or remove directories to be monitored (they must be comma separated). All files and subdirectories will also be monitored. Drive letters without directories are not valid. At a minimum the '.' should be included (`D:\.`). This should be set on the system you wish to monitor (or in the agent.conf if appropriate).

Default: /etc,/usr/bin,/usr/sbin,/bin,/sbin

Attributes:

- **realtime**: Value=yes
  - This will enable realtime/continuous monitoring on Linux (using the inotify system calls) and Windows systems.
- **report_changes**: Value=yes
  - Report diffs of file changes. This is limited to text files at this time.

Note: This option is only available on Unix-like systems.

- **check_all**: Value=yes
  - All the following check_* options are used together.
- **check_sum**: Value=yes
  - Check the md5 and sha1 hashes of the of the files will be checked.

    This is the same as using both check_sha1sum="yes" and check_md5sum="yes"
- **check_sha1sum**: Value=yes
  - When used only the sha1 hash of the files will be checked.
- **check_md5sum**: Value=yes
  - The md5 hash of the files will be checked.
- **check_size**: Value=yes
  - The size of the files will be checked.
- **check_owner**: Value=yes
  - Check the owner of the files selected.
- **check_group**: Value=yes
  - Check the group owner of the files/directories selected.
- **check_perm**: Value=yes
  - Check the UNIX permission of the files/directories selected. On windows this will only check the POSIX permissions.
- **restrict**: Value=string
  - A string that will limit checks to files containing that string in the file name.

    Allowed: Any directory or file name (but not a path)

ignore
List of files or directories to be ignored (one entry per element). The files and directories are still checked, but the results are ignored.

Default: /etc/mtab

Attributes:

- **type**: Value=sregex
  - This is a simple regex pattern to filter out files so alerts are not generated.

Allowed: Any directory or file name

frequency
Frequency that the syscheck is going to be executed (in seconds).

The default is 6 hours or 21600 seconds

Default: 21600

Allowed: Time in seconds

scan_time
Time to run the scans (can be in the formats of 21pm, 8:30, 12am, etc)

Allowed: Time to run scan

scan_day
Day of the week to run the scans (can be in the format of sunday, saturday, monday, etc)

Allowed: Day of the week

auto_ignore
Specifies if syscheck will ignore files that change too often (after the third change)

Default: yes

Allowed: yes/no

Valid: server, local

alert_new_files
Specifies if syscheck should alert on new files created.

Default: no

Allowed: yes/no

Valid: server, local

Note: New files will only be detected on a full scan, this option does not work in realtime.

---

scan_on_start
Specifies if syscheck should do the first scan as soon as it is started.

Default: yes

Allowed: yes/no

windows_registry
Use this option to add Windows registry entries to be monitored (Windows-only).

Default: HKEY_LOCAL_MACHINESoftware

Allowed: Any registry entry (one per element)

Note: New entries will not trigger alerts, only changes to existing entries.

registry_ignore
List of registry entries to be ignored.

Default: ..CryptographyRNG

Allowed: Any registry entry (one per element)

refilter_cmd
Command to run to prevent prelinking from creating false positives.

Example:

```
<prefilter_cmd>/usr/sbin/prelink -y</prefilter_cmd>
```

Note: This option can potentially impact performance negatively. The configured command will be run for each and every file checked.

ospatrol.conf: Syslog Output options

Overview

Supported types Syslog Output options are available in the the following installation types:

- server
- local

Location All syslog_output options must be configured in the /var/ospatrol/etc/ospatrol.conf and used within the <ospatrol_config> tag.

XML excerpt to show location:

```
<ospatrol_config>
    <syslog_output>
        <!--
        Syslog Output options here
        -->
    </syslog_output>
</ospatrol_config>
```

Options

syslog_output

server

•IP Address of the syslog server.

•**Allowed:** any valid IP address

port

•Port to forward alerts to.

•**Default** 514

- **Allowed:** Any valid port

level

- Alert level of the alerts to forward.
- **Allowed:** 1 - 16

group

- Alerts belonging to this group will be forwarded.
- **Allowed:** Any valid group. Separate multiple groups with the pipe (|) character.
- **Examples:**

```
<group>syscheck</group>
<group>authentication_failure|authentication_success</group>
```

rule_id

- Alerts matching this rule_id will be forwarded.
- **Allowed:** Any valid rule_id

location

- Alerts from this location will be forwarded.
- **Allowed:** Any valid logfile location

format

- Format of alert output. The default format is "default", or full syslog output.
- CEF is the ArcSight Common Event Format.
- json can be used with a variety of tools.
- The splunk option is for sending data to a Splunk server.
- **Allowed** default, cef, splunk, json

```
<syslog_output>
  <server>10.0.0.1</server>
  <port>514</port>
  <format>cef</format>
</syslog_output>
```

2.1.4 agent.conf

Overview

More information on using the agent.conf can be found here

Supported types

The agent.conf is valid on the server install only.

Location

The `agent.conf` exists in `/var/ospatrol/etc/shared`. It should be readable by the ospatrol user.

XML excerpt to show location:

```
<agent_config>
    ...
</agent_config>
```

Options

agent_config_options

agent_config
Defines the beginning or end of an agent configuration block.

name

This option to `agent_config` allows you to assign the block the one particular agent by using the agent's name.

Example: <agent_config name="agent007">

os

This option to `agent_config` allows you to assign the block to an operating system.

Example: <agent_config os="Windows">

Allowed: Any OS family (Windows, Linux, OpenBSD, etc.)

profile

This option to `agent_config` allows you to assign a profile name to the the block. Any agent may use this block if it is configured to use the defined profile.

Example: <agent_config profile="webservers">

2.1.5 internal_options.conf: syntax and options

internal_options.conf: analysisd

analysisd.default_timeframe
Analysisd default rule timeframe

Default: 360

Allowed: Any interger

analysisd.stats_maxdiff
Default: 25000

Allowed: Any interger

analysisd.stats_mindiff
Default: 250

Allowed: Any interger

analysisd.stats_percent_diff
Default: 30

Allowed: Any interger

analysisd.fts_list_size
Default: 32

Allowed: Any interger

analysisd.fts_min_size_for_str
Default: 14

Allowed: Any interger

analysisd.log_fw
Default: 1

Allowed: Any interger

analysisd.debug
Default: 0

Allowed: Any interger

internal_options.conf: agent

agent.debug
Run the agent's processes in debug mode.

Default: 0

internal_options.conf: dbd

dbd.reconnect_attempts
The number of times `ospatrol-dbd` will attempt to reconnect to the database.

Default: 10

internal_options.conf: logcollector

logcollector.loop_timeout
Default: 2

logcollector.open_attempts
Default: 8

logcollector.remote_commands=0
Allow the agents to run commands defined in `agent.conf`.

Allowed: 0,1

Default: 0

Note: This option first appeared in OSPatrol 2.7.

---

internal_options.conf: maild

maild.strict_checking
Default: 1

Allowed: 0 or 1

maild.groupping
If set to `1` alerts will be grouped together in one email. These alerts may be of different types or levels, and may be from different systems.

Default: 1

Allowed: 0 or 1

maild.full_subject
If set to `1` maild will use a full subject when sending alert emails. If set to `0` the subject is shortened.

Default: 0

Allowed: 0 or 1

maild.geoip
If set to `1` mails will display GeoIP data in alert emails.

Default: 1

Allowed: 0 or 1

internal_options.conf: monitord

monitord.day_wait
Amount of time OSPatrol will wait before compressing/signing log files.

Default: 10

monitord.compress
If set to `1` `ospatrol-monitord` will compress old log files.

Default: 1

Available: 0 or 1

monitord.sign
If set to `1` `ospatrol-monitord` will sign old log files.

Default: 1

monitord.monitor_agents
Default: 1

internal_options.conf: remoted

remoted.recv_counter_flush
Default: 128

remoted.comp_average_printout
Default: 19999

remoted.verify_msg_id
Default: 1

remoted.debug
Default: 0

internal_options.conf: syscheck

syscheck.sleep
`ospatrol-syscheckd` uses this setting to determine how long to sleep after reading `syscheck.sleep_after` number of files. By default `ospatrol-syscheckd` sleeps for 2 seconds after checking 15 files.

Default: 2

syscheck.sleep_after
`ospatrol-syscheckd` reads this many files before sleeping for `syscheck.sleep` seconds.

Default: 15

internal_options.conf: windows

windows.debug
Default: 0 **Allowed:** 0 or 1

2.2 Man pages

2.2.1 agent-auth

The agent-auth program is the client application used with *ospatrol-authd* to automatically add agents to an OSPatrol manager.

agent-auth argument options

-h
Display the help message

-m `<manager_ip>`
IP address of the manager.

-p `<port>`
Port ospatrol-authd is running on. **Default** 1515

-A `<agent_name>`
Agent name to be used. **Default** hostname

-D
Directory where OSPatrol is installed. **Default** /var/ospatrol

agent-auth example usage

Example: Adding an agent with a hostname

```
# /var/ospatrol/bin/agent-auth -m 192.168.1.1 -p 1515 -A example-agent
INFO: Connected to 192.168.1.1:1515
INFO: Using agent name as: melancia
INFO: Send request to manager. Waiting for reply.
INFO: Received response with agent key
INFO: Valid key created. Finished.
INFO: Connection closed.
```

2.2.2 agent_control

The agent_control tool allows you to query and get information from any agent you have configured on your server and it also allows you to restart (run now) the syscheck/rootcheck scan on any agent.

Enabling active response will be necessary to start scans remotely and possibly other functions.

agent_control argument options

-h
Display the help message

-l
List available (active or not) agents

-lc
List active agents

-i <agent_id>
Extracts information from an agent

-R <agent_id>
Restarts the OSPatrol processes on the agent

Note: Requires active response to be enabled.

-r
Run the integrity/rootcheck checking on agents. Must be utilized with *agent_control -a* or *agent_control -u*

Note: Requires active response to be enabled.

-a
Utilizes all agents.

-u <agent_id>
<agent_id> that will perform the requested action.

agent_control example usage

Example 1: Listing all active agents

The first interesting argument is *agent_control -lc*, to list the connected (active agents). To list all of them, use *agent_control -l* only.

```
# /var/ospatrol/bin/agent_control -lc
OSPatrol HIDS agent_control. List of available agents:
ID: 000, Name: enigma.ospatrol.net (server), IP: 127.0.0.1, Active/Local
ID: 002, Name: winhome, IP: 192.168.2.190, Active
ID: 005, Name: jul, IP: 192.168.2.0/24, Active
ID: 165, Name: esqueleto2, IP: 192.168.2.99, Active
ID: 174, Name: lili3win, IP: 192.168.2.0/24, Active
```

Example 2: Querying information from agent 002

To query an agent, just use the *agent_control -i* option followed by the agent id.

```
# /var/ospatrol/bin/agent_control -i 002

OSPatrol HIDS agent_control. Agent information:
Agent ID: 002
Agent Name: winhome
IP address: 192.168.2.190
Status: Active

Operating system: Microsoft Windows XP Professional (Build 2600)
Client version: OSPatrol HIDS v1.5-SNP-080412
Last keep alive: Fri Apr 25 14:33:03 2008

Syscheck last started at: Fri Apr 25 05:07:13 2008
Rootcheck last started at: Fri Apr 25 09:04:12 2008
```

Example 3: Executing syscheck and rootcheck scan immediately

To execute the syscheck/rootcheck scan immediately, use the *agent_control -r* option followed by the *agent_control -u* with the agent id.

```
# /var/ospatrol/bin/agent_control -r -u 000

OSPatrol HIDS agent_control: Restarting Syscheck/Rootcheck locally.
```

2.2.3 clear_stats

Clear the events stats

clear_stats argument options

-h
: Print and display a help message of all available options to clear_stats

-a
: Clear all the stats (averages).

-d
: Clear the daily averages.

-w
: Clear the weekly averages.

2.2.4 list_agents

OSPatrol HIDS list_agents: List available agents.

list_agents is only available on OSPatrol servers or local mode installations. It can be used to retrieve

- a list of all OSPatrol agents that successfully connected to the server in the past
- a list of all OSPatrol agents currently connected to the server
- a list of all OSPatrol agents that were connected to the server in the past but are currently not connected.

If an agent was added via the *manage_agents* tool but has not yet been connected to the server, it will not show up in the output of list_agents.

list_agents argument options

-h
Display the help message.

-a
List all agents.

-c
List the connected (active) agents.

-n
List the not connected (active) agents.

2.2.5 manage_agents

manage_agents is available in two versions:

- a version for OSPatrol server installations
- a version for OSPatrol agent installations

The purpose of manage_agents is to provide an easy-to-use interface to handle authentication keys for OSPatrol agents. These authentication keys are required for secure (encrypted and authenticated) communication between the OSPatrol server and its affiliated agent instances.

manage_agents argument options

-h
Display the help message.

-V
Display OSPatrol Version.

-l
List available agents.

-e `<agent_id>`
Extracts key for an agent (Manager only).

-i `<key>`
Import authentication key (Agent only).

-f <file>
Generate clients in bulk from <file> (Manager only). The file is a comma delimited file containing the IP addresses and agent names to be added. This file should be located within /var/ospatrol, and referenced by its path relative to /var/ospatrol.

Example:

```
# cat /var/ospatrol/k
192.168.1.2,host02
192.168.1.3,host03

# /var/ospatrol/bin/manage_agents -f /k
Bulk load file: /k
Opening: [/k]
Agent information:
   ID:002
   Name:host02
   IP Address:192.168.1.2

Agent added.
Agent information:
   ID:003
   Name:host03
   IP Address:192.168.1.3

Agent added.
```

Usage

The OSPatrol manual goes into details on usage of this command at *Managing Agents*

2.2.6 ospatrol-agentd

ospatrol-agentd is the client side daemon that communicates with the server. It runs as ospatrol and is chrooted to /var/ospatrol by default.

ospatrol-agentd argument options

-d
Run in debug mode.

-V
Version and license information.

-h
Display the help message.

-t
Test configuration.

-f
Run ospatrol-agentd in the foreground.

-u <user>
Run ospatrol-agentd as <user>.

Default: ospatrolm

-g <group>
Run ospatrol-agentd as <group>.

-c <config>
Run ospatrol-agentd using <config> as the configuration file.

Default: /var/ospatrol/etc/ospatrol.conf

-D <dir>
Chroot to <dir>.

Default: /var/ospatrol

2.2.7 ospatrol-agentlessd

2.2.8 ospatrol-analysisd

ospatrol-analysisd recveives the log messages and compares them to the rules. It will create alerts when a log message matches an applicable rule.

ospatrol-analysisd argument options

-V
Version and license message

-h
Help message.

-d
Execute in debug mode

-t
Test configuration

-c <config>
Configuration file ospatrol-analysisd should use

-D <dir>
Chroot to <dir>

2.2.9 ospatrol-authd

The ospatrol-authd daemon will automatically add an agent to an OSPatrol manager and provide the key to the agent. The *agent-auth* application is the client application used with ospatrol-authd. *ospatrol-authd* will create an agent with an ip address of *any* instead of using its actual IP.

There is no authentication involved in this transaction, so it is recommended that this daemon only be run when a new agent is being added.

ospatrol-authd argument options

-d
Run in debug mode.

-i
Add agents with a specific IP address instead of using any.

-p <port>
Listen on port.

Default 1515

Creating SSL keys

ospatrol-authd requires SSL keys to run. This process will create the necessary keys in /var/ospatrol/etc and allow ospatrol-authd to start:

```
# openssl genrsa -out /var/ospatrol/etc/sslmanager.key 2048
# openssl req -new -x509 -key /var/ospatrol/etc/sslmanager.key -out /var/ospatrol/etc/sslmanager.cert
```

Without the key ospatrol-authd will give the following error:

```
[user@ospatrol-manager] :; sudo /var/ospatrol/bin/ospatrol-authd
2012/04/18 11:05:01 ospatrol-authd: INFO: Started (pid: 20669).
2012/04/18 11:05:01 ospatrol-authd: ERROR: Unable to read certificate file (not found): /var/ospatrol
2012/04/18 11:05:01 ospatrol-authd: ERROR: SSL error. Exiting.
```

ospatrol-authd example usage

Example: Running ospatrol-authd

```
# /var/ospatrol/bin/ospatrol-authd -p 1515 >/dev/null 2>&1 &
```

And the logs when an agent is added:

```
2011/01/19 15:04:40 ospatrol-authd: INFO: New connection from 192.168.10.5
2011/01/19 15:04:41 ospatrol-authd: INFO: Received request for a new agent (example-agent) from: 192.
2011/01/19 15:04:41 ospatrol-authd: INFO: Agent key generated for example-agent (requested by 192.168.
2011/01/19 15:04:41 ospatrol-authd: INFO: Agent key created for example-agent (requested by 192.168.1
```

2.2.10 ospatrol-control

ospatrol-control is a script to start, stop, configure, or check on the status of OSPatrol processes. ossc-control can enable or disable client-syslog, database logging, agentless configurations, and debug mode.

ospatrol-control argument options

start Start the OSPatrol processes.

stop Stop the OSPatrol processes.

restart Restart the OSPatrol processes.

reload Restart all OSPatrol processes except ospatrol-execd. This allows an agent to reload without losing active response status.

Note: This is only available on an OSPatrol agent.

---

status Determine which OSPatrol processes are running.

enable Enable OSPatrol functionality.

database Enable the `ospatrol-dbd` daemon for logging to a database.

Available: Server and local installs only.

Note: Database support must be compiled in at install time.

client-syslog Enable `ospatrol-csyslogd` for logging to remote syslog.

Available: Server and local installs only.

agentless Enable `ospatrol-agentlessd` for running commands on systems without OSPatrol agents.

Available: Server and local installs only.

debug Run all OSPatrol daemons in debug mode.

disable Disable OSPatrol functionality.

database Disable the `ospatrol-dbd` daemon for logging to a database.

Available: Server and local installs only.

Note: Database support must be compiled in at install time.

client-syslog

Disable `ospatrol-csyslogd` for logging to remote syslog.

Available: Server and local installs only.

agentless Disable `ospatrol-agentlessd` for running commands on systems without OSPatrol agents.

Available: Server and local installs only.

debug Turn off debug mode.

ospatrol-control example usage

Example: Running ospatrol-control

```
# /var/ospatrol/bin/ospatrol-control

Usage: /var/ospatrol/bin/ospatrol-control {start|stop|restart|status|enable|disable}
```

2.2.11 ospatrol-csyslogd

`ospatrol-csyslogd` is a daemon that forwards the OSPatrol alerts via syslog. Configuration is done in the `<syslog_output>` section of the ospatrol.conf. (see *ospatrol.conf: Syslog Output options*)

ospatrol-csyslogd argument options

-d
Run in debug mode.

-v
Version and license information.

-h
Display the help message.

-t
Test configuration.

-f
Run `ospatrol-csyslogd` in the foreground.

-u <user>
Run `ospatrol-csyslogd` as <user>.

Default: ospatrolm

-g <group>
Run `ospatrol-csyslogd` as <group>.

-c <config>
Run `ospatrol-csyslogd` using <config> as the configuration file.

Default: /var/ospatrol/etc/ospatrol.conf

-D <dir>
Chroot to <dir>.

Default: /var/ospatrol

2.2.12 ospatrol-dbd

The `ospatrol-dbd` daemon inserts the alert logs into a database, either postgresql or mysql. `ospatrol-dbd` is configured in ospatrol.conf. (see *ospatrol.conf: Database Output options*)

ospatrol-dbd argument options

-d
Run in debug mode.

-V
Version and license information.

-h
Display the help message.

-t
Test configuration.

-f
Run `ospatrol-dbd` in the foreground.

-u <user>
Run `ospatrol-dbd` as <user>.

Default: ospatrolm

-g <group>
Run `ospatrol-dbd` as <group>.

-c <config>
Run `ospatrol-dbd` using <config> as the configuration file.

Default: /var/ospatrol/etc/ospatrol.conf

-D <dir>
Chroot to <dir>.

Default: /var/ospatrol

2.2.13 ospatrol-execd

`ospatrol-execd` executes active responses by running the configured scripts. `ospatrol-execd` is configured in the ospatrol.conf. (see *ospatrol.conf: Active Response Options*)

ospatrol-execd argument options

-d
Run in debug mode.

-V
Version and license information.

-h
Display the help message.

-t
Test configuration.

-f
Run `ospatrol-execd` in the foreground.

-c <config>
Run `ospatrol-execd` using <config> as the configuration file.

Default: /var/ospatrol/etc/ospatrol.conf

-D <dir>
Chroot to <dir>.

Default: /var/ospatrol

2.2.14 ospatrol-logcollector

The `ospatrol-logcollector` daemon monitors configured files and commands for new log messages. `ospatrol-logcollector` is configured in ospatrol.conf. (see *ospatrol.conf: Localfile options*)

ospatrol-logcollector argument options

-d
Run in debug mode.

-V
Version and license information.

-h
Display the help message.

-t
Test configuration.

-f
Run `ospatrol-logcollector` in the foreground.

-c <config>
Run `ospatrol-logcollector` using <config> as the configuration file.

Default: /var/ospatrol/etc/ospatrol.conf

-D <dir>
Chroot to <dir>.

Default: /var/ospatrol

2.2.15 ospatrol-logtest

ospatrol-logtest is the single most useful tool when working with ospatrol. This tool allows oneself to test and verify log files in the exact same way that *ospatrol-anaylistd* does.

Something ospatrol-logtest can help with:

- Writing rules (Debugging your custom rules)
- Troubleshooting false positives or false negatives

ospatrol-logtest accepts standard input for all log to test.

osssec-logtest argument options

-d
Print debug output to the terminal.

-V
Print the Version and license message for OSPatrol and ospatrol-logtest.

-h
Print the help message to the console.

-t
Test configuration. This will print file details on the ospatrol-anaylistd rules, decoders, and lists as they are loaded and the order they were processed.

-v
Full output of all details and matches.

Note: This the key argument to troubleshoot a rule, decoder problem.

Note: This is argument was incorrectly displayed as running in the foreground in all version before version 2.5

-u <user>
Run as <user>: ospatrol-logtest will change uid to the user specified as part of this argument.

Often used with *ospatrol-logtest -g*

-g <group>
Run as <group>: ospatrol-logtest will change gid to the group specified as part of this argument.

Often used with *ospatrol-logtest -u*

-c <config>
<config> is the path and filename to load in place of the default /var/ospatrol/etc/ospatrol.conf.

-D <dir>
: This is the path that ospatrol-logtest will chroot to before it completes loading all rules, decoders, and lists and processing standard input.

-a
: Analyze of input lines as if they are live events.

Caveats

Some log formats will be processed differently than they appear in the log file. MySQL log files for instance will have ‘‘MySQL log: ‘‘ prepended to the log message before analysis. If using ospatrol-logtest to test MySQL logs, please add this string to the beginning.

Example:

Given the following MySQL log message:

```
130218 12:07:52 [Warning] Unsafe statement written to the binary log using statement format since BIN
```

The message that should be pasted into ospatrol-logtest is:

```
MySQL log: 130218 12:07:52 [Warning] Unsafe statement written to the binary log using statement forma
```

ospatrol-logtest example usage

Example 1: Testing standard rules

```
# echo "Aug 29 15:33:13 ns3 named[464]: client 217.148.39.3#1036: query (cache) denied" | /var/ospatr
2010/08/10 06:57:06 ospatrol-testrule: INFO: Reading decoder file loadables/decoders/00_decoders.xml.
2010/08/10 06:57:06 ospatrol-testrule: INFO: Reading decoder file loadables/decoders/50_named.xml.
2010/08/10 06:57:06 ospatrol-testrule: INFO: Reading decoder file loadables/decoders/50_pam.xml.
2010/08/10 06:57:06 ospatrol-testrule: INFO: Reading decoder file loadables/decoders/50_sshd.xml.
2010/08/10 06:57:06 ospatrol-testrule: INFO: Reading loading the lists file: 'loadables/lists/rfc1918
2010/08/10 06:57:06 ospatrol-testrule: INFO: Started (pid: 78828).
ospatrol-testrule: Type one log per line.



**Phase 1: Completed pre-decoding.
       full event: 'Aug 29 15:33:13 ns3 named[464]: client 217.148.39.3#1036: query (cache) denied'
       hostname: 'ns3'
       program_name: 'named'
       log: 'client 217.148.39.3#1036: query (cache) denied'

**Phase 2: Completed decoding.
       decoder: 'named'
       srcip: '217.148.39.3'

**Rule debugging:
    Trying rule: 1 - Generic template for all syslog rules.
       *Rule 1 matched.
       *Trying child rules.
    Trying rule: 30100 - Apache messages grouped.
    Trying rule: 7200 - Grouping of the arpwatch rules.
    Trying rule: 6200 - Asterisk messages grouped.
    Trying rule: 9600 - cimserver messages grouped.
```

```
    Trying rule: 4700 - Grouping of Cisco IOS rules.
    Trying rule: 3900 - Grouping for the courier rules.
    Trying rule: 9700 - Dovecot Messages Grouped.
    Trying rule: 11100 - Grouping for the ftpd rules.
    Trying rule: 9300 - Grouping for the Horde imp rules.
    Trying rule: 3600 - Grouping of the imapd rules.
    Trying rule: 3700 - Grouping of mailscanner rules.
    Trying rule: 3800 - Grouping of Exchange rules.
    Trying rule: 6300 - Grouping for the MS-DHCP rules.
    Trying rule: 6350 - Grouping for the MS-DHCP rules.
    Trying rule: 11500 - Grouping for the Microsoft ftp rules.
    Trying rule: 50100 - MySQL messages grouped.
    Trying rule: 12100 - Grouping of the named rules
       *Rule 12100 matched.
       *Trying child rules.
    Trying rule: 12107 - DNS update using RFC2136 Dynamic protocol.
    Trying rule: 12101 - Invalid DNS packet. Possibility of attack.
    Trying rule: 12109 - Named fatal error. DNS service going down.
    Trying rule: 12102 - Failed attempt to perform a zone transfer.
    Trying rule: 12103 - DNS update denied. Generally mis-configuration.
    Trying rule: 12104 - Log permission misconfiguration in Named.
    Trying rule: 12105 - Unexpected error while resolving domain.
    Trying rule: 12106 - DNS configuration error.
    Trying rule: 12108 - Query cache denied (maybe config error).
       *Rule 12108 matched.

**Phase 3: Completed filtering (rules).
       Rule id: '12108'
       Level: '4'
       Description: 'Query cache denied (maybe config error).'
       Info - Link: 'http://www.reedmedia.net/misc/dns/errors.html'
**Alert to be generated.
```

Example 2: Using OSPatrol for the forensic analysis of log files

If you have one old log file that you want to check or if you are doing a forensics analysis of a box and wants to check the logs with OSPatrol, we now have a solution too.

Let's say you have a file /var/log/secure that you want to analyze with OSPatrol. You need to use the ospatrol-logtest tool with the "-a" flag to reproduce the alerts:

```
# cat /var/log/secure | /var/ospatrol/bin/ospatrol-logtest -a

** Alert 1264788284.11: - syslog,sshd,authentication_success,
2010 Jan 29 14:04:44 enigma->stdin
Rule: 5715 (level 3) -> 'SSHD authentication success.'
Src IP: a.b.2.15
User: dcid
Jan 15 10:25:01 enigma sshd[17594]: Accepted password for dcid from a.b.2.15 port 47526 ssh2

** Alert 1264788284.12: - syslog,sshd,authentication_success,
2010 Jan 29 14:04:44 enigma->stdin
Rule: 5715 (level 3) -> 'SSHD authentication success.'
Src IP: 127.0.0.1
User: dcid
Jan 15 11:19:20 enigma sshd[18853]: Accepted publickey for dcid from 127.0.0.1 port 6725 ssh2
```

You will get the alerts just like you would at /var/ospatrol/logs/alerts.log. The benefit now is that you can pipe this output to *ospatrol-reported* to get a better view of what is going on:

```
# cat /var/log/secure | /var/ospatrol/bin/ospatrol-logtest -a |/var/ospatrol/bin/ospatrol-reported
Report completed. ==
--------------------------------
->Processed alerts: 522
->Post-filtering alerts: 522

Top entries for 'Source ip':
--------------------------------
89.200.169.170 |41 |
127.0.0.1 |33 |
83.170.106.142 |20 |
204.232.206.109 |16 |
..

Top entries for 'Username':
--------------------------------
root |247 |

Top entries for 'Level':
--------------------------------
Severity 5 |406 |
Severity 3 |41 |
Severity 10 |32 |

Top entries for 'Group':
--------------------------------
syslog |522 |
sshd |509 |
authentication_failed |369 |
invalid_login |146 |

Top entries for 'Rule':
--------------------------------
5716 - SSHD authentication failed. |223 |
5710 - Attempt to login using a non-existent.. |146 |
5715 - SSHD authentication success. |41 |
5702 - Reverse lookup error (bad ISP or atta.. |37 |
```

To get a report of all brute force attacks (for example) that scanned my box:

```
# cat /var/log/secure | /var/ospatrol/bin/ospatrol-logtest -a |/var/ospatrol/bin/ospatrol-reported -f

Report completed. ==
--------------------------------
->Processed alerts: 522
->Post-filtering alerts: 25

Top entries for 'Source ip':
--------------------------------
83.170.106.142 |2 |
89.200.169.170 |2 |
114.255.100.163 |1 |
117.135.138.183 |1 |
124.205.62.36 |1 |
173.45.108.230 |1 |
200.182.99.59 |1 |
```

```
202.63.160.50 |1 |
210.21.225.202 |1 |
211.151.64.220 |1 |
213.229.70.12 |1 |
218.30.19.48 |1 |
221.12.12.3 |1 |
59.3.239.114 |1 |
61.168.227.12 |1 |
61.233.42.47 |1 |
67.43.61.80 |1 |
72.52.75.228 |1 |
77.245.148.196 |1 |
79.125.35.214 |1 |
85.21.83.170 |1 |
92.240.75.6 |1 |
94.198.49.185 |1 |

Top entries for 'Username':
--------------------------------
root |24 |

Top entries for 'Level':
--------------------------------
Severity 10 |25 |

Top entries for 'Group':
--------------------------------
authentication_failures |25 |
sshd |25 |
syslog |25 |

Top entries for 'Location':
--------------------------------
enigma->stdin |25 |

Top entries for 'Rule':
--------------------------------
5720 - Multiple SSHD authentication failures. |24 |
5712 - SSHD brute force trying to get access.. |1 |
```

2.2.16 ospatrol-maild

The `ospatrol-maild` daemon sends OSPatrol alerts via email. `ospatrol-maild` is started by ospatrol-control. Configuration for ospatrol-maild is handled in the ospatrol.conf. (see *ospatrol.conf: Global options*)

ospatrol-maild argument options

-d
: Run in debug mode.

-V
: Version and license information.

-h
: Display the help message.

-t
Test configuration.

-f
Run `ospatrol-maild` in the foreground.

-u <user>
Run `ospatrol-maild` as <user>.

Default: ospatrolm

-g <group>
Run `ospatrol-maild` as <group>.

-c <config>
Run `ospatrol-maild` using <config> as the configuration file.

Default: /var/ospatrol/etc/ospatrol.conf

-D <dir>
Chroot to <dir>.

Default: /var/ospatrol

2.2.17 ospatrol-makelists

The `ospatrol-makelists` utility to compile cdb databases. `ospatrol-makelists` will scan ospatrol.conf for database files, check the mtime, and recompile all out of date databases.

See *CDB List lookups from within Rules* for more information.

ospatrol-makelists argument options

-h
Display the help message.

-V
Diplay the version and license information.

-d
Execute in debug mode.

-f
Force rebuild of all databases.

-u <user>
Run as <user>.

-g <group>
Run as <group>.

-c <config>
Run with configuration file of <config>.

Default /var/ospatrol/etc/ospatrol.conf

-D <dir>
Chroot to <dir>.

Default /var/ospatrol

ospatrol-makelists example usage

Example: Running ospatrol-makelists and an update is necessary

```
# /var/ospatrol/bin/ospatrol-makelists
 * File lists/blocked.txt.cdb need to be updated
```

Example: Running ospatrol-makelists when no update is necessary

```
# /var/ospatrol/bin/ospatrol-makelists
 * File lists/blocked.txt.cdb does not need to be compiled
```

2.2.18 ospatrol-monitord

The `ospatrol-monitord` daemon monitors agent connectivity and compress daily log files. `ospatrol-monitord` is configured in ospatrol.conf. (see *ospatrol.conf: Localfile options*)

ospatrol-monitord argument options

-d
Run in debug mode.

-V
Version and license information.

-h
Display the help message.

-t
Test configuration.

-f
Run `ospatrol-monitord` in the foreground.

-u `<user>`
Run `ospatrol-monitord` as <user>.

Default: ospatrolm

-g `<group>`
Run `ospatrol-monitord` as <group>.

-c `<config>`
Run `ospatrol-monitord` using <config> as the configuration file.

Default: /var/ospatrol/etc/ospatrol.conf

-D `<dir>`
Chroot to <dir>.

Default: /var/ospatrol

2.2.19 ospatrol-regex

‘‘ospatrol-regex‘ is a simple program that will validate a regex expression.a The pattern should be enclosed in single quotes to help prevent any strange interactions with the shell.

The syntax for `ospatrol-regex` is simple: `/var/ospatrol/bin/ospatrol-regex '<pattern>'` It then reads strings from stdin and outputs matches to stdout. `+OSRegex_Execute` and `+OS_Regex` are printed if a match is successful.

Example 1: A siple digit match:

```
# /var/ospatrol/bin/ospatrol-regex '^\d\d\d'
333
+OSRegex_Execute: 333
+OS_Regex       : 333
f44
222
+OSRegex_Execute: 222
+OS_Regex       : 222
```

2.2.20 ospatrol-remoted

`ospatrol-remoted` is the server side daemon that communicates with the agents. It can listen to port 1514/udp (for OSPatrol communications) and/or 514 (for syslog). It runs as ospatrolr and is chrooted to `/var/ospatrol` by default. `ospatrol-remoted` is configured in the <remote> section of ospatrol.conf. (see *ospatrol.conf: Remote Options*)

ospatrol-remoted argument options

-d
Run in debug mode.

-V
Version and license information.

-h
Display the help message.

-t
Test configuration.

-u `<user>`
Run `ospatrol-remoted` as <user>.

Default: ospatrolm

-g `<group>`
Run `ospatrol-remoted` as <group>.

-c `<config>`
Run `ospatrol-remoted` using <config> as the configuration file.

Default: /var/ospatrol/etc/ospatrol.conf

-D `<dir>`
Chroot to <dir>.

Default: /var/ospatrol

2.2.21 ospatrol-reportd

`ospatrol-reportd` is a program to create reports from OSPatrol alerts. `ospatrol-reportd` accepts alerts on `stdin`, and outputs a report on `stderr`.

Note: Since `ospatrol-reportd` outputs to stderr some utilities like `less` will not work if you do not redirect the output. End the ospatrol-reportd with `2>&1` to redirect stderr to stdout. `more` or `less` can be easily used after the stderr redirect.

---

ospatrol-reportd argument options

-h
Display the help message

-f `<filter> <value>`
Filter the results.

-r `<filter> <value>`
Show related entries.

-n `<string>`
Create a description for the report.

-s
Show the alerts related to the summary.

ospatrol-reportd example usage

Example 1: Show Successful Logins

```
# cat /var/ospatrol/logs/alerts/alerts.log | /var/ospatrol/bin/ospatrol-reportd -f group authenticati
```

Example 2: Show Alerts Level 10 and Greater

```
# cat /var/ospatrol/logs/alerts/alerts.log | /var/ospatrol/bin/ospatrol-reportd -f level 10
```

Example 3: Show the srcip for all users

```
# cat /var/ospatrol/logs/alerts/alerts.log | /var/ospatrol/bin/ospatrol-reportd -f group authenticati
```

Example 4: Show Changed files as reported by Syscheck

```
# cat /var/ospatrol/logs/alerts/alerts.log | /var/ospatrol/bin/ospatrol-reportd -f group syscheck -r
```

Example output

```
# cat /var/ospatrol/logs/alerts/alerts.log | /var/ospatrol/bin/ospatrol-reportd 2>&1 | more
2011/07/11 21:01:36 ospatrol-reportd: INFO: Started (pid: 1444).
2011/07/11 21:01:41 ospatrol-reportd: INFO: Report completed. Creating output...

Report completed. ==
-------------------------------------------------
->Processed alerts: 17
->Post-filtering alerts: 17
->First alert: 2011 Jul 11 00:00:46
->Last alert: 2011 Jul 11 00:16:52


Top entries for 'Username':
-------------------------------------------------
_nrpe                                            |6       |
SYSTEM                                           |2       |


Top entries for 'Level':
-------------------------------------------------
Severity 3                                       |13      |
Severity 2                                       |4       |


Top entries for 'Group':
-------------------------------------------------
syslog                                           |10      |
sudo                                             |6       |
dropbearrecon                                    |4       |
ospatrol                                            |4       |
sshd                                             |4       |
authentication_success                           |2       |
windows                                          |2       |
clamd                                            |1       |
freshclam                                        |1       |
virus                                            |1       |


Top entries for 'Location':
-------------------------------------------------
ix->/var/log/secure                              |4       |
ix->ospatrol-logcollector                           |3       |
(vistapc) 192.168.17.0->WinEvtLog                |2       |
buffalo1->/var/log/secure                        |2       |
buffalo2->/var/log/secure                        |2       |
(junction) 192.168.17.17->/var/log/secure        |1       |
(junction) 192.168.17.17->ospatrol-logcollector     |1       |
ix->/var/log/local6                              |1       |
junction->/var/log/secure                        |1       |


Top entries for 'Rule':
-------------------------------------------------
5402 - Successful sudo to ROOT executed          |6       |
51006 - Client exited before authentication.     |4       |
591 - Log file rotated.                          |4       |
```

```
18107 - Windows Logon Success.                  |2       |
52507 - ClamAV database update                  |1       |
```

2.2.22 ospatrol-syscheckd

The `ospatrol-syscheckd` daemon checks configured files for changes to the checksums, permissions or ownership. `ospatrol-syscheckd` is started by ospatrol-control. Configuration for ospatrol-syscheckd is handled in the ospatrol.conf.

See *Syscheck* for more detailed configuration information.

ospatrol-syscheckd argument options

-d
Run in debug mode.

-V
Version and license information.

-h
Display the help message.

-t
Test configuration.

-f
Run `ospatrol-syscheckd` in the foreground.

-c `<config>`
Run `ospatrol-syscheckd` using <config> as the configuration file.

Default: /var/ospatrol/etc/ospatrol.conf

-D `<dir>`
Chroot to <dir>.

Default: /var/ospatrol

2.2.23 rootcheck_control

The rootcheck_control tool allows you to manage the policy monitoring and system auditing database that is stored on the server (manager) side. You can list anomalies detected by the rootcheck functionality, categorized into resolved and outstanding issues. Moreover you can find out when ospatrol-rootcheck was run the last time.

rootcheck_control argument options

-h
Display the help message.

-l
List available agents.

-lc
List only currently connected agents.

-u <id>
Updates (clear) the database for the agent.

-u all
Updates (clear) the database for all agents.

-i <agent_id>
Prints database for the agent.

-r
Used with -i, prints all the resolved issues.

-q
Used with -i, prints all the outstanding issues.

-L
Used with -i, prints the last scan.

-s
Changes the output to CSV (comma delimited).

rootcheck_control example usage

Example 1: Getting a list of system auditing/policy monitoring events

To get a list of all auditing/policy monitoring events for a specific agent, you can run *rootcheck_control -i*. To retrieve the agent id you can use any of the following commands:

- *rootcheck_control -l*,
- *agent_control -l*
- *syscheck_control -l*
- *syscheck_update -l*
- *manage_agents -l*

```
# /var/ospatrol/bin/rootcheck_control -i 002

Policy and auditing events for agent 'ospatrolagent (002) - 192.168.1.86':

Resolved events:

2010 Jun 15 13:01:22 (first time detected: 2009 Dec 10 18:48:43)
System Audit: System Audit: CIS - Debian Linux 8.8 - GRUB Password not set. File: /boot/grub/menu.lst


Outstanding events:

2010 Jun 17 17:34:37 (first time detected: 2009 Dec 10 18:48:43)
System Audit: System Audit: CIS - Testing against the CIS Debian Linux Benchmark v1.0. File: /etc/deb

2010 Jun 17 17:34:37 (first time detected: 2009 Dec 10 18:48:43)
System Audit: System Audit: CIS - Debian Linux 1.4 - Robust partition scheme - /tmp is not on its own

2010 Jun 17 17:34:37 (first time detected: 2009 Dec 10 18:48:43)
System Audit: System Audit: CIS - Debian Linux 2.3 - SSH Configuration - Root login allowed. File: /e
```

As you can see the detected events are shown in two categories, resolved events and outstanding event. To only show resolved events, run *rootcheck_control -ri*. To only show outstanding events, run *rootcheck_control -ri*. To only show the results of the last scan and time of that scan, run *rootcheck_control -Li*.

To gain that kind of information for the OSPatrol server, run *rootcheck_control -i 000*.

Example 2: Clearing the system auditing/policy database

To clear the system auditing/policy monitoring database for a certain agent run the following command:

```
# /var/ospatrol/bin/rootcheck_control -u 002

** Policy and auditing database updated.
```

To clear the database for all agents and the server run the following command:

```
# /var/ospatrol/bin/rootcheck_control -u all

** Policy and auditing database updated.
```

The next time rootcheck is run, the database will be populated again.

2.2.24 syscheck_control

syscheck_control provides an interface for managing and viewing the integrity checking database.

syscheck_control argument options

-h
Display the help message.

-l
List available agents.

-lc
List only currently connected agents.

-u <agent_id>
Updates (clear) the database for the agent.

-u all
Updates (clear) the database for all agents.

-i <agent_id>
Prints database for the agent.

-r -i
List modified registry entries for the agent (Windows only).

-f <file>
Used with -i. Prints information about a modified file.

-z
Used with -f, zeroes the auto-ignore counter.

-d
Used with -f, ignores that file.

-s
Changes the output to CSV (comma delimited).

syscheck_control example usage

Example 1: Getting a list of modified files for an agent

To retrieve information about files that were monitored by OSPatrol and modified after OSPatrol was deployed, run *syscheck_control -i*.

```
# /var/ospatrol/bin/syscheck_control -i 002

Integrity changes for agent 'ospatrol-agent (002) - 192.168.1.86':

Changes for 2009 Dec 21:
2009 Dec 21 13:52:40,0 - /etc/authorization
2009 Dec 21 13:52:42,0 - /etc/cups/printers.conf
2009 Dec 21 13:52:42,0 - /etc/cups/printers.conf.O
2009 Dec 21 13:52:58,0 - /etc/postfix/main.cf.default

Changes for 2010 Jan 04:
2010 Jan 04 10:13:58,0 - /etc/authorization

Changes for 2010 Jan 06:
2010 Jan 06 09:45:43,0 - /etc/postfix/main.cf.default

Changes for 2010 Jan 18:
2010 Jan 18 09:18:51,0 - /etc/cups/printers.conf
2010 Jan 18 09:18:51,0 - /etc/cups/printers.conf.O

Changes for 2010 Feb 23:
2010 Feb 23 09:17:22,2 - /etc/cups/printers.conf
2010 Feb 23 09:17:22,2 - /etc/cups/printers.conf.O

Changes for 2010 Mar 24:
2010 Mar 24 08:42:52,3 - /etc/cups/printers.conf
2010 Mar 24 08:42:52,3 - /etc/cups/printers.conf.O
```

As you can see this command provides an overview about file modifications.

Example 2: Getting more detailed information about a modified file

If you need to get more detailed information about a file that was modified you can use syscheck_control to view

- the time stamp when the file was added to the syscheck database
- the integrity checking values when the file was added to the syscheck database
- the time stamps when OSPatrol detected a modification
- the integrity checking values for every time OSPatrol detected a modification.

The integrity checking values include

- how often the file has changed
- file size
- file permissions

- owner and group id of the file
- MD5 and SHA1 hashes of the file.

To retrieve this information, run *syscheck_control -i*:

```
# /var/ospatrol/bin/syscheck_control -i 002 -f /etc/authorization

Integrity changes for agent 'ospatrol-agent (002) - 192.168.1.86':
Detailed information for entries matching: '/etc/authorization'

2009 Dec 21 13:52:40,0 - /etc/authorization
File added to the database.
Integrity checking values:
   Size: 27771
   Perm: rw-r--r--
   Uid:  0
   Gid:  0
   Md5:  dd62912576ae05d611d7469be809cf1d
   Sha1: 530df0283df52f0152b9e7ce1a518119b06ceebc

2010 Jan 04 10:13:58,0 - /etc/authorization
File changed. - 1st time modified.
Integrity checking values:
   Size: >28050
   Perm: rw-r--r--
   Uid:  0
   Gid:  0
   Md5:  >50da55def41bcede7d42ac5ee8fe12c9
   Sha1: >97f4b2b48a97321a3e245221e0ea4353cf4fa8ef
```

Example 3: Clearing the syscheck database

To clear the syscheck database for a certain agent run the following command:

```
# /var/ospatrol/bin/syscheck_control -u 002

** Integrity check database updated.
```

syscheck_control -i 002 will now show that no modified files for that agent are in the database:

```
# /var/ospatrol/bin/syscheck_control -i 002

Integrity changes for agent 'ospatrol-agent (002) - 192.168.1.86':

** No entries found.
```

To clear the database for all agents and the server run the following command:

```
# /var/ospatrol/bin/syscheck_control -u all

** Integrity check database updated.
```

The next time syscheck is run, the database will be populated again.

2.2.25 syscheck_update

syscheck_update: Updates the integrity check database. This means that all information about files that were added to the integrity check database will be dismissed and leave an empty database which will be populated again the next time the syscheck daemon runs on agents or the server.

It does the same thing as *syscheck_control -u '(cf. :ref: 'syscheck_control*).

syscheck_update argument options

-h
Display the help message.

-l
List available agents.

-a
Updates the database for all agents.

-u <agent_id>
Updates the database for the agent.

-u local
Updates the local database.

2.2.26 util.sh

The `util.sh` script can add a file to be monitored by `ospatrol-logcollector`. It can also add a full_command to check for changes to a website, or for changes to the name server of a domain.

A blogpost from Daniel Cid (for 3WoO) introduced this utility.

util.sh argument options

addfile <filename> [<format>]
Add a file to be monitored by `ospatrol-logtest`. A `localfile` will be added to the ospatrol.conf.

addsite <domain>
Monitor a website for changes. A `full_command` will be added to the `ospatrol.conf` using lynx to dump the initial page. A rule can be written to monitor this output for changes.

Note: Requires lynx.

Warning: This may not be useful on pages with dynamic content.

adddns <domain>
Monitor the name server of a domain for changes. A `full_command` will be added to the ospatrol.conf using host

---

Note: Requites the `host` command.

---

util.sh example usage

Example: Running util.sh

Running the following command:

```
# /var/ospatrol/bin/util.sh adddns ospatrol.net
```

will add the folling to that system's `ospatrol.conf`:

```
<ospatrol_config>
   <localfile>
     <log_format>full_command</log_format>
     <command>host -W 5 -t NS ospatrol.net; host -W 5 -t A ospatrol.net | sort</command>
   </localfile>
 </ospatrol_config>
```

2.2.27 verify-agent-conf

`verify-agent-conf` verifies the OSPatrol agent.conf configuration. It exits silently if the configuration is correct.

verify-agent-conf example usage

Example 1: Running verify-agent-conf on a working agent.conf

```
# /var/ospatrol/bin/verify-agent-conf
#
```

Example 2: Running verify-agent-conf on a non-working agent.conf

```
# /var/ospatrol/bin/verify-agent-conf
2011/07/12 21:22:07 ospatrol-config(1226): ERROR: Error reading XML file '/var/ospatrol/etc/shared/ag
```

2.3 Rules/Decoders Documentation

Contents:

2.3.1 Rules Documentation

Contents:

2.4 Rootcheck / Syscheck Reference

2.4.1 Information about the Beastkit Rootkit

This rootkit was found on a RedHat 7.2 System in 01/2002. The rootkit setup script includes the line "#Beastkit 7.0 - X-Org edition". Due to this fact, we call it as "Beastkit 7.0".

More Information

For more info, look at this analyse (author unknown): *analysis-beastkit*

Files

- `usr/include/rpc/ ../kit`
- `usr/include/rpc/ ../kit2`
- `usr/doc/.sl`
- `usr/doc/.sp`
- `usr/doc/.statnet`
- `usr/doc/.logdsys`
- `usr/doc/.dpct`
- `usr/doc/.gifnocfi`
- `usr/doc/.dnif`
- `usr/doc/.nigol`
- `*biba`
- `*sniff/lins`

Note: All files with an "*" need to be search in all system

If you have any more Information about this rootkits sent to rootkits at ossec.net

2.4.2 Information about the Knark Rootkit

Knark is a kernel-based rootkit for Linux 2.2/2.4. It hide ports, files and processes from the administrator. This rootkit is very powerfull and had been used by "crackers" in a lot of compromised machines.

More Information

- A complete analysis, done by Toby Miller, can be found here: *analysis-knack*
- Knark README can be found *readme-knack*
- Download: http://www.ossec.net/rootkits/files/knark-2.4.3.tgz MD5: ca1ebe26ab1138ebe431751f526df817

Files

- `/dev/.pizda`
- `/dev/.pula`
- `/proc/knark`
- `*/taskhack`
- `*/rootme`
- `*/nethide`

- */hidef
- */ered

Note: All files with an "*" need to be search in all system

If you have any more Information about this rootkits sent to rootkits at ossec.net

2.4.3 Information about Old Rootkits

These "Old Rootkits" are some old (obvious) rootkits, found in some systems years ago. They are not very well documented and because of that we call them only as "Old".

Files

- usr/include/rpc/ ../kit
- usr/include/rpc/ ../kit2
- usr/doc/.sl
- usr/doc/.sp
- usr/doc/.statnet
- usr/doc/.logdsys
- usr/doc/.dpct
- usr/doc/.gifnocfi
- usr/doc/.dnif
- usr/doc/.nigol
- *biba
- *sniff/lins

Note: All files with an "*" need to be search in all system

If you have any more Information about this rootkits sent to rootkits at ossec.net

2.4.4 Information about Suspicious files

The files listed here were found in some infected/owned machines. They are not part of any rootkit, but some "crackers" use them. They can be a log of some sniffer, a sniffer or a lot of other things.

Take a careful look if you find any of these files in your system.

More Information

N/A

Origin of Rule

N/A

File

- etc/rc.d/init.d/rc.modules
- lib/ldd.so
- usr/man/muie
- usr/X11R6/include/pain
- usr/bin/sourcemask
- usr/bin/ras2xm
- usr/bin/ddc
- usr/bin/jdc
- usr/sbin/in.telnet
- sbin/vobiscum
- usr/sbin/jcd
- usr/sbin/atd2
- usr/bin/ishit
- usr/bin/.etc
- usr/bin/xstat
- var/run/.tmp
- usr/man/man1/lib/.lib
- usr/man/man2/.man8
- var/run/.pid
- lib/.so
- lib/.fx
- lib/lblip.tk
- usr/lib/.fx
- var/local/.lpd
- dev/rd/cdb
- dev/.rd/
- usr/lib/pt07
- usr/bin/atm
- tmp/.cheese
- dev/.arctic
- dev/.xman
- dev/srd0
- dev/ptyzx
- dev/ptyzg
- dev/xdf1

- dev/ttyop
- dev/ttyof
- dev/hd5
- dev/hd6
- dev/hd7
- dev/hdx1
- dev/hdx2
- dev/xdf2
- dev/ptyp
- dev/ptyr
- */.src
- *last.cgi
- *nobody.cgi
- *void.cgi
- *all4one.cgi
- *xntps
- */.xman
- */.arctic
- *psybnc
- *mech.session
- *sshdu

Note: All files with an "*" need to be search in all system

If you have any more Information about this rootkits sent to rootkits at ossec.net

2.4.5 Information about the T.R.K rootkit

This rootkit as a mix of some others.

More Information

No more information is available.

Orgin of Rule

This rootkit was taken from chkrootkit:

```
### T.R.K
expertmode_output "${find} ${ROOTDIR}usr/bin -name soucemask -o -name ct"
```

File

- `usr/bin/soucemask`
- `usr/bin/sourcemask`

Note: All files with an "*" need to be search in all system

If you have any more Information about this rootkits sent to rootkits at ossec.net

2.4.6 Information about the Tuxkit Rootkit

This is a rootkit written by a Dutch group called Tuxtendo. It was found in some infected Redhat 6.0/7.0 systems.

More Information

A complete analyse of Tuxkit, done by Spoonfork (spoonfork@hackinthebox.org). For more info, look at this analyse (author unknown): *analysis-tuxkit*

Files

– `dev/tux` – `usr/bin/xsf` – `usr/bin/xchk` – `*/.log` – `*/.file` – `*/.addr`

Entries to search on file "/etc/rc.d/rc.sysinit":

– `/usr/bin/xsf` – `/usr/bin/xchk`

Note: All files with an "*" need to be search in all system

If you have any more Information about this rootkits sent to rootkits at ossec.net

2.5 Log Samples

2.5.1 Stuff

Apache Logs

Log Samples from Apache

Apache generally has two log files: apache error log and apache access log.
 The format of these files can be changed in the configuration, but these are
 the default formats:

Apache access log (success - code 200):

```
192.168.2.20 - - [28/Jul/2006:10:27:10 -0300] "GET /cgi-bin/try/ HTTP/1.0" 200 3395
127.0.0.1 - - [28/Jul/2006:10:22:04 -0300] "GET / HTTP/1.0" 200 2216
```

Apache access log (failure - code 4xx):

```
127.0.0.1 - - [28/Jul/2006:10:27:32 -0300] "GET /hidden/ HTTP/1.0" 404 7218
```

Apache unnacepted request methods (caused by TortoiseSVN):

```
x.x.x.90 - - [13/Sep/2006:07:01:53 -0700] "PROPFIND /svn/[xxxx]/Extranet/branches/SOW-101 HTTP/1.1" 4
x.x.x.90 - - [13/Sep/2006:07:01:51 -0700] "PROPFIND /svn/[xxxx]/[xxxx]/trunk HTTP/1.1" 401 587
x.x.x.90 - - [13/Sep/2006:07:00:53 -0700] "PROPFIND /svn/[xxxx]/[xxxx]/2.5 HTTP/1.1" 401 587
x.x.x.90 - - [13/Sep/2006:07:00:53 -0700] "PROPFIND /svn/[xxxx]/Extranet/branches/SOW-101 HTTP/1.1" 4
x.x.x.90 - - [13/Sep/2006:07:00:21 -0700] "PROPFIND /svn/[xxxx]/[xxxx]/trunk HTTP/1.1" 401 587
x.x.x.90 - - [13/Sep/2006:06:59:53 -0700] "PROPFIND /svn/[xxxx]/[xxxx]/2.5 HTTP/1.1" 401 587
x.x.x.90 - - [13/Sep/2006:06:59:50 -0700] "PROPFIND /svn/[xxxx]/[xxxx]/trunk HTTP/1.1" 401 587
x.x.x.90 - - [13/Sep/2006:06:58:52 -0700] "PROPFIND /svn/[xxxx]/[xxxx]/trunk HTTP/1.1" 401 587
x.x.x.90 - - [13/Sep/2006:06:58:52 -0700] "PROPFIND /svn/[xxxx]/Extranet/branches/SOW-101 HTTP/1.1" 4
```

Apache error log:

```
[Fri Dec 16 01:46:23 2005] [error] [client 1.2.3.4] Directory index forbidden by rule: /home/test/
[Fri Dec 16 01:54:34 2005] [error] [client 1.2.3.4] Directory index forbidden by rule: /apache/web-da
[Fri Dec 16 02:25:55 2005] [error] [client 1.2.3.4] Client sent malformed Host header
[Mon Dec 19 23:02:01 2005] [error] [client 1.2.3.4] user test: authentication failure for "/~dcid/tes
```

Apache error log (startup) 3 examples:

```
** Normal (v2.x)
[Sat Aug 12 04:05:51 2006] [notice] Apache/1.3.11 (Unix) mod_perl/1.21 configured -- resuming normal
[Thu Jun 22 14:20:55 2006] [notice] Digest: generating secret for digest authentication ...
[Thu Jun 22 14:20:55 2006] [notice] Digest: done
[Thu Jun 22 14:20:55 2006] [notice] Apache/2.0.46 (Red Hat) DAV/2 configured -- resuming normal opera

** Restart by HUP signal (optional suEXEC)
[Sat Aug 12 04:05:49 2006] [notice] SIGHUP received.  Attempting to restart
[Sat Aug 12 04:05:51 2006] [notice] suEXEC mechanism enabled (wrapper: /usr/local/apache/sbin/suexec)

** after 'unclean' shutdown (left over PID file)
[Sat Jun 24 09:06:22 2006] [warn] pid file /opt/CA/BrightStorARCserve/httpd/logs/httpd.pid overwritte
[Sat Jun 24 09:06:23 2006] [notice] Apache/2.0.46 (Red Hat) DAV/2 configured -- resuming normal opera
[Sat Jun 24 09:06:22 2006] [notice] Digest: generating secret for digest authentication ...
[Sat Jun 24 09:06:22 2006] [notice] Digest: done
```

Apache error log (shutdown by TERM signal):

```
[Thu Jun 22 11:35:48 2006] [notice] caught SIGTERM, shutting down
```

Apache without resources:

```
[Tue Mar 08 10:34:21 2005] [error] (11)Resource temporarily unavailable: fork: Unable to fork new pro
[Tue Mar 08 10:34:31 2005] [error] (11)Resource temporarily unavailable: fork: Unable to fork new pro
```

Apache Attack samples

Mambo attacks and their patterns in the apache access log file.

```
193.91.75.11 - - [18/Aug/2006:13:23:13 -0300] "GET /index.php?_REQUEST[option]=com_content&_REQUEST[
```

```
212.227.132.51 - - [18/Aug/2006:05:24:07 -0300] "GET /index.php?_REQUEST[option]=com_content&_REQUEST
```

```
201.226.254.210 - - [18/Aug/2006:13:47:46 -0300] "GET /index.php?_REQUEST[option]=com_content&_REQUES

212.227.132.51 - - [18/Aug/2006:13:56:29 -0300] "GET /index.php?_REQUEST[option]=com_content&_REQUEST

62.103.159.21 - - [18/Aug/2006:13:58:02 -0300] "GET /index.php?_REQUEST[option]=com_content&_REQUEST
```

PHPBB attacks and their patterns in the apache access log file.

```
 207.36.232.148 - - [28/Aug/2006:07:08:46 -0300] "GET /index.php/Artigos/modules/Forums/admin/admin_u

193.255.143.5 - - [28/Aug/2006:07:52:45 -0300] "GET /index.php/modules/Forums/admin/admin_users.php?p
```

SQL injection attempt on PHP Nuke

```
200.96.104.241 - - [12/Sep/2006:09:44:28 -0300] "GET /modules.php?name=Downloads&d_op=modifydownloadr
```

Night of scans

```
[17/Dec/2005:02:40:45 -0500] - - 85.226.238.xxx "GET /awstats/awstats.pl?configdir=|echo;echo%20YYY;c
[17/Dec/2005:02:40:46 -0500] - - 85.226.238.xxx "GET /cgi-bin/awstats.pl?configdir=|echo;echo%20YYY;c
[17/Dec/2005:02:40:47 -0500] - - 85.226.238.xxx "GET /cgi-bin/awstats/awstats.pl?configdir=|echo;echo
[17/Dec/2005:02:40:48 -0500] - - 85.226.238.xxx "GET /index2.php?option=com_content&do_pdf=1&id=1inde
[17/Dec/2005:02:40:49 -0500] - - 85.226.238.xxx "GET /index.php?option=com_content&do_pdf=1&id=1index
[17/Dec/2005:02:40:50 -0500] - - 85.226.238.xxx "GET /mambo/index2.php?_REQUEST[option]=com_content&_
[17/Dec/2005:02:40:52 -0500] - - 85.226.238.xxx "GET /cvs/index2.php?_REQUEST[option]=com_content&_RE
[17/Dec/2005:02:40:53 -0500] - - 85.226.238.xxx "GET /cvs/mambo/index2.php?_REQUEST[option]=com_conte
[17/Dec/2005:03:07:04 -0500] - - 24.19.40.xxx "GET /awstats/awstats.pl?configdir=|echo;echo%20YYY;cd%
[17/Dec/2005:04:34:04 -0500] - - 64.105.82.xxx "GET /blogtest/xmlsrv/xmlrpc.php HTTP/1.1" "-" 302 336
[17/Dec/2005:05:18:40 -0500] - - 195.82.6.xxx "GET /modules/Forums/admin/admin_styles.phpadmin_styles
[17/Dec/2005:05:18:41 -0500] - - 195.82.6.xxx "GET /Forums/admin/admin_styles.phpadmin_styles.php?php
[17/Dec/2005:05:18:43 -0500] - - 195.82.6.xxx "POST /xmlrpc.php HTTP/1.1" "-" 302 336 0
[17/Dec/2005:05:18:45 -0500] - - 195.82.6.xxx "POST /blog/xmlrpc.php HTTP/1.1" "-" 302 336 0
[17/Dec/2005:05:18:47 -0500] - - 195.82.6.xxx "POST /blog/xmlsrv/xmlrpc.php HTTP/1.1" "-" 302 336 0
[17/Dec/2005:05:18:48 -0500] - - 195.82.6.xxx "POST /blogs/xmlsrv/xmlrpc.php HTTP/1.1" "-" 302 336 1
[17/Dec/2005:05:18:50 -0500] - - 195.82.6.xxx "POST /drupal/xmlrpc.php HTTP/1.1" "-" 302 336 0
[17/Dec/2005:05:18:52 -0500] - - 195.82.6.xxx "POST /phpgroupware/xmlrpc.php HTTP/1.1" "-" 302 336 0
[17/Dec/2005:05:18:54 -0500] - - 195.82.6.xxx "POST /wordpress/xmlrpc.php HTTP/1.1" "-" 302 336 0
[17/Dec/2005:05:18:55 -0500] - - 195.82.6.xxx "POST /xmlrpc.php HTTP/1.1" "-" 302 336 0
[17/Dec/2005:05:18:57 -0500] - - 195.82.6.xxx "POST /xmlrpc/xmlrpc.php HTTP/1.1" "-" 302 336 0
[17/Dec/2005:05:18:59 -0500] - - 195.82.6.xxx "POST /xmlsrv/xmlrpc.php HTTP/1.1" "-" 302 336 0
[17/Dec/2005:09:14:57 -0500] - - 81.186.243.xxx "GET /modules/Forums/admin/admin_styles.phpadmin_styl
[17/Dec/2005:09:14:58 -0500] - - 81.186.243.xxx "GET /Forums/admin/admin_styles.phpadmin_styles.php?p
[17/Dec/2005:09:14:59 -0500] - - 81.186.243.xxx "POST /xmlrpc.php HTTP/1.1" "-" 302 336 1
[17/Dec/2005:09:15:00 -0500] - - 81.186.243.xxx "POST /blog/xmlrpc.php HTTP/1.1" "-" 302 336 1
[17/Dec/2005:09:15:02 -0500] - - 81.186.243.xxx "POST /blog/xmlsrv/xmlrpc.php HTTP/1.1" "-" 302 336 1
[17/Dec/2005:09:15:03 -0500] - - 81.186.243.xxx "POST /blogs/xmlsrv/xmlrpc.php HTTP/1.1" "-" 302 336
[17/Dec/2005:09:15:05 -0500] - - 81.186.243.xxx "POST /drupal/xmlrpc.php HTTP/1.1" "-" 302 336 0
[17/Dec/2005:09:15:05 -0500] - - 81.186.243.xxx "POST /phpgroupware/xmlrpc.php HTTP/1.1" "-" 302 336
[17/Dec/2005:09:15:06 -0500] - - 81.186.243.xxx "POST /wordpress/xmlrpc.php HTTP/1.1" "-" 302 336 1
[17/Dec/2005:09:15:08 -0500] - - 81.186.243.xxx "POST /xmlrpc.php HTTP/1.1" "-" 302 336 1
[17/Dec/2005:09:15:09 -0500] - - 81.186.243.xxx "POST /xmlrpc/xmlrpc.php HTTP/1.1" "-" 302 336 1
[17/Dec/2005:09:15:10 -0500] - - 81.186.243.xxx "POST /xmlsrv/xmlrpc.php HTTP/1.1" "-" 302 336 1
[17/Dec/2005:09:45:55 -0500] - - 69.65.151.xxx "PROPFIND / HTTP/1.0" "-" 403 332 0
```

```
201-67-28-XXX.bsace703.dsl.brasiltelecom.net.br - - [16/Sep/2006:15:18:53 -0300] "GET /cursosuperior/
201-67-28-XXX.bsace703.dsl.brasiltelecom.net.br - - [16/Sep/2006:15:51:59 -0300] "GET /cursosuperior/
```

GNU Radius

Information on GNU Radius can be found here.

Information on the detailed accounting in GNU Radius can be found here.

Here is a sample of the accounting records taken from the above documentation:

```
Fri Dec 15 18:00:24 2000
      Acct-Session-Id = "2193976896017"
      User-Name = "e2"
      Acct-Status-Type = Start
      Acct-Authentic = RADIUS
      Service-Type = Framed-User
      Framed-Protocol = PPP
      Framed-IP-Address = 11.10.10.125
      Calling-Station-Id = "+15678023561"
      NAS-IP-Address = 11.10.10.11
      NAS-Port-Id = 8
      Acct-Delay-Time = 0
      Timestamp = 976896024
      Request-Authenticator = Unverified

Fri Dec 15 18:32:09 2000
      Acct-Session-Id = "2193976896017"
      User-Name = "e2"
      Acct-Status-Type = Stop
      Acct-Authentic = RADIUS
      Acct-Output-Octets = 5382
      Acct-Input-Octets = 7761
      Service-Type = Framed-User
      Framed-Protocol = PPP
      Framed-IP-Address = 11.10.10.125
      Acct-Session-Time = 1905
      NAS-IP-Address = 11.10.10.11
      NAS-Port-Id = 8
      Acct-Delay-Time = 0
      Timestamp = 976897929
      Request-Authenticator = Unverified
```

Windows Routing and Remote Access logs

This sample is in the Microsoft IAS Database Compatible log format (text file). A description of this format is found **'here http://www.microsoft.com/windows2000/en/server/help/sag_ias_log2a.htm>'_** and here

```
"RasBox","RAS",10/22/2006,09:13:09,1,"ACME\slimjim","ACME\slimjim",,,,,,"192.168.132.45",12,,"192.168
"RasBox","RAS",10/22/2006,09:13:09,3,,"ACME\slimjim",,,,,,,,,,,,,,,,4,,36,"311 1 192.168.132.45 07/3
"RasBox","RAS",10/22/2006,09:13:13,1,"ACME\slimjim","ACME\slimjim",,,,,,"192.168.132.45",12,,"192.168
"RasBox","RAS",10/22/2006,09:13:13,3,,"ACME\slimjim",,,,,,,,,,,,,,,,4,,36,"311 1 192.168.132.45 07/3
"RasBox","RAS",10/22/2006,09:13:21,1,"ACME\slimjim","ACME\slimjim",,,,,,"192.168.132.45",12,,"192.168
"RasBox","RAS",10/22/2006,09:13:21,3,,"ACME\slimjim",,,,,,,,,,,,,,,,4,,36,"311 1 192.168.132.45 07/3
```

```
"RasBox","RAS",10/22/2006,09:14:37,1,"ACME\slimjim","ACME\slimjim",,,,,,"192.168.132.45",12,,"192.168
"RasBox","RAS",10/22/2006,09:14:37,1,"ACME\slimjim","ACME\slimjim",,,,,,"192.168.132.45",12,,"192.168
"RasBox","RAS",10/22/2006,09:14:37,3,,"ACME\slimjim",,,,,,,,,,,,,,,,4,,36,"311 1 192.168.132.45 07/3
"RasBox","RAS",10/22/2006,11:57:11,1,"ACME\megaman","ACME\megaman",,,,,,"192.168.132.45",13,,"192.168
"RasBox","RAS",10/22/2006,11:57:11,3,,"ACME\megaman",,,,,,,,,,,,,,,,4,,16,"311 1 192.168.132.45 07/3
"RasBox","RAS",10/22/2006,11:57:54,1,"ACME\megaman","acme.net/Users/megaman",,,,,,"192.168.132.45",13
```

You can find information on the IAS standard log format here and here

Log Samples from Pam

Logs from PAM_Unix can be in different formats depending on the operating system. It can cause a lot of trouble when parsing it.

The available formats are:

```
process_name(pam_unix)[pid]:
process_name[pid]: (pam_unix)
process_name: pam_unix(process_name):
```

Login sucessful:

```
Jul  7 10:51:24 srbarriga su(pam_unix)[14592]: session opened for user test2 by (uid=10101)
Jul  7 10:52:14 srbarriga sshd(pam_unix)[17365]: session opened for user test by (uid=508)
Nov 17 21:41:22 localhost su[8060]: (pam_unix) session opened for user root by (uid=0)
Nov 11 22:46:29 localhost vsftpd: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=
```

Session closed:

```
Jul  7 10:53:07 srbarriga su(pam_unix)[14592]: session closed for user test
```

Login failed:

```
Jul  7 10:55:56 srbarriga sshd(pam_unix)[16660]: authentication failure; logname= uid=0 euid=0 tty=NO
Jul  7 10:59:12 srbarriga vsftpd(pam_unix)[25073]: authentication failure; logname= uid=0 euid=0 tty=
```

Invalid user login attempt:

```
Jul  7 10:59:49 srbarriga vsftpd(pam_unix)[25073]: check pass; user unknown
```

Log Samples from sshd

If the system is using pam, authentication events from sshd may also be logged in the pam format

Always make sure to disable DNS lookup to have the IP address logged instead of the hostname (sshd_config):

```
UseDNS no
```

Did not receive identification string (occurs during some forms of sshd DoS):

```
Mar  8 06:08:23 stamina sshd[7713]: Did not receive identification string from 190.97.xx.199
Mar  8 06:08:26 stamina sshd[7758]: Did not receive identification string from 190.97.xx.199
Mar  8 06:08:26 stamina sshd[7739]: Did not receive identification string from 190.97.xx.199
Mar  8 06:08:27 stamina sshd[7770]: Did not receive identification string from 190.97.xx.199
```

Rule to catch multiple instances (insert into local_rules.xml):

```
<rule id="100031" level="10" frequency="4" timeframe="360">
  <if_matched_sid>5706</if_matched_sid>
  <description>Possible DDoS attempt </description>
  <description>(high number of non-existent identification strings).</description>
</rule>
```

Software caused connection abort (occurs during some forms of sshd DoS):

```
Mar  8 06:09:56 stamina sshd[82181]: error: accept: Software caused connection abort
Mar  8 06:13:11 stamina sshd[82181]: error: accept: Software caused connection abort
Mar  8 06:13:42 stamina sshd[82181]: error: accept: Software caused connection abort
```

Rule to help OSSEC recognise this error as nothing serious:

Login sucessful:

```
May 21 20:22:28 slacker2 sshd[8813]: Accepted password for root from 192.168.20.185 port 1066 ssh2
May 21 20:22:28 sol2 sshd[23857]: [ID 702911 auth.notice] User test1, coming from 192.168.2.185,  -
Oct 11 08:05:46 hostname auth|security:info sshd[323808]: Accepted publickey for usr1 from 2.3.4.5 po
```

Login failed:

```
May 21 20:22:28 slacker sshd[21487]: Failed password for root from 192.168.20.185 port 1045 ssh2
```

Invalid user login attempt:

```
Jul  7 10:51:24 chaves sshd[19537]: Invalid user admin from spongebob.lab.ossec.net
Jul  7 10:53:24 chaves sshd[12914]: Failed password for invalid user test-inv from spongebob.lab.osse
Jul  7 10:53:24 kiko sshd[3251]: User dcid not allowed because listed in DenyUsers
```

Full scan sample:

```
Aug  1 18:27:45 knight sshd[20325]: Illegal user test from 218.49.183.17
Aug  1 18:27:46 knight sshd[20325]: Failed password for illegal user test from 218.49.183.17 port 488
Aug  1 18:27:46 knight sshd[20325]: error: Could not get shadow information for NOUSER
Aug  1 18:27:48 knight sshd[20327]: Illegal user guest from 218.49.183.17
Aug  1 18:27:49 knight sshd[20327]: Failed password for illegal user guest from 218.49.183.17 port 49
Aug  1 18:27:49 knight sshd[20327]: error: Could not get shadow information for NOUSER
Aug  1 18:27:52 knight sshd[20329]: Failed password for admin from 218.49.183.17 port 49266 ssh2
Aug  1 18:27:56 knight sshd[20331]: Failed password for admin from 218.49.183.17 port 49468 ssh2
Aug  1 18:27:58 knight sshd[20334]: Illegal user user from 218.49.183.17
Aug  1 18:27:59 knight sshd[20334]: Failed password for illegal user user from 218.49.183.17 port 496
Aug  1 18:27:59 knight sshd[20334]: error: Could not get shadow information for NOUSER
Aug  1 18:28:02 knight sshd[20336]: Failed password for root from 218.49.183.17 port 49869 ssh2
Aug  1 18:28:05 knight sshd[20347]: Failed password for root from 218.49.183.17 port 50063 ssh2
Aug  1 18:28:12 knight sshd[20349]: Failed password for root from 218.49.183.17 port 50245 ssh2
Aug  1 18:28:14 knight sshd[20352]: Illegal user test from 218.49.183.17
Aug  1 18:28:19 knight sshd[20352]: Failed password for illegal user test from 218.49.183.17 port 506
Aug  1 18:28:19 knight sshd[20352]: error: Could not get shadow information for NOUSER
Aug  1 18:29:55 knight sshd[20402]: Illegal user test from 218.49.183.17
Aug  1 18:29:56 knight sshd[20402]: Failed password for illegal user test from 218.49.183.17 port 522
Aug  1 18:29:56 knight sshd[20402]: error: Could not get shadow information for NOUSER
Aug  1 18:29:58 knight sshd[20404]: Illegal user guest from 218.49.183.17
Aug  1 18:30:02 knight sshd[20406]: Illegal user test from 218.49.183.17
Aug  1 18:30:03 knight sshd[20404]: Failed password for illegal user guest from 218.49.183.17 port 52
Aug  1 18:30:03 knight sshd[20404]: error: Could not get shadow information for NOUSER
Aug  1 18:30:03 knight sshd[20406]: Failed password for illegal user test from 218.49.183.17 port 525
Aug  1 18:30:03 knight sshd[20406]: error: Could not get shadow information for NOUSER
Aug  1 18:30:05 knight sshd[20439]: Failed password for illegal user guest from 218.49.183.17 port 52
Aug  1 18:30:05 knight sshd[20439]: Illegal user guest from 218.49.183.17
Aug  1 18:30:05 knight sshd[20439]: error: Could not get shadow information for NOUSER
Aug  1 18:30:06 knight sshd[20441]: Failed password for admin from 218.49.183.17 port 52851 ssh2
Aug  1 18:30:08 knight sshd[20443]: Failed password for admin from 218.49.183.17 port 53014 ssh2
Aug  1 18:30:09 knight sshd[20445]: Failed password for admin from 218.49.183.17 port 53040 ssh2
Aug  1 18:30:11 knight sshd[20447]: Failed password for admin from 218.49.183.17 port 53192 ssh2
Aug  1 18:30:11 knight sshd[20449]: Illegal user user from 218.49.183.17
Aug  1 18:30:12 knight sshd[20449]: Failed password for illegal user user from 218.49.183.17 port 532
Aug  1 18:30:12 knight sshd[20449]: error: Could not get shadow information for NOUSER
Aug  1 18:30:13 knight sshd[20451]: Illegal user user from 218.49.183.17
Aug  1 18:30:14 knight sshd[20451]: Failed password for illegal user user from 218.49.183.17 port 534
Aug  1 18:30:14 knight sshd[20451]: error: Could not get shadow information for NOUSER
Aug  1 18:30:14 knight sshd[20453]: Failed password for root from 218.49.183.17 port 53425 ssh2
Aug  1 18:30:21 knight sshd[20455]: Failed password for root from 218.49.183.17 port 53571 ssh2
Aug  1 18:30:22 knight sshd[20457]: Failed password for root from 218.49.183.17 port 53615 ssh2
Aug  1 18:30:24 knight sshd[20476]: Failed password for root from 218.49.183.17 port 54033 ssh2
Aug  1 18:30:24 knight sshd[20484]: Failed password for root from 218.49.183.17 port 54078 ssh2
Aug  1 18:30:26 knight sshd[20488]: Illegal user test from 218.49.183.17
Aug  1 18:30:27 knight sshd[20486]: Failed password for root from 218.49.183.17 port 54243 ssh2
Aug  1 18:30:27 knight sshd[20488]: Failed password for illegal user test from 218.49.183.17 port 542
Aug  1 18:30:27 knight sshd[20488]: error: Could not get shadow information for NOUSER
Aug  1 18:30:29 knight sshd[20490]: Illegal user test from 218.49.183.17
Aug  1 18:30:34 knight sshd[20490]: Failed password for illegal user test from 218.49.183.17 port 544
Aug  1 18:30:34 knight sshd[20490]: error: Could not get shadow information for NOUSER
Aug  1 18:35:53 knight sshd[20658]: Illegal user test from 218.49.183.17
Aug  1 18:35:54 knight sshd[20658]: Failed password for illegal user test from 218.49.183.17 port 396
Aug  1 18:35:54 knight sshd[20658]: error: Could not get shadow information for NOUSER
Aug  1 18:35:56 knight sshd[20660]: Illegal user guest from 218.49.183.17
Aug  1 18:35:57 knight sshd[20660]: Failed password for illegal user guest from 218.49.183.17 port 39
Aug  1 18:35:57 knight sshd[20660]: error: Could not get shadow information for NOUSER
Aug  1 18:36:00 knight sshd[20664]: Failed password for admin from 218.49.183.17 port 40009 ssh2
```

```
Aug  1 18:36:04 knight sshd[20666]: Failed password for admin from 218.49.183.17 port 40217 ssh2
Aug  1 18:36:06 knight sshd[20675]: Illegal user user from 218.49.183.17
Aug  1 18:36:11 knight sshd[20675]: Failed password for illegal user user from 218.49.183.17 port 404
Aug  1 18:36:11 knight sshd[20675]: error: Could not get shadow information for NOUSER
Aug  1 18:36:14 knight sshd[20677]: Failed password for root from 218.49.183.17 port 40973 ssh2
Aug  1 18:36:21 knight sshd[20679]: Failed password for root from 218.49.183.17 port 41159 ssh2
Aug  1 18:36:24 knight sshd[20681]: Failed password for root from 218.49.183.17 port 41541 ssh2
Aug  1 18:36:27 knight sshd[20683]: Illegal user test from 218.49.183.17
Aug  1 18:36:28 knight sshd[20683]: Failed password for illegal user test from 218.49.183.17 port 416
Aug  1 18:36:28 knight sshd[20683]: error: Could not get shadow information for NOUSER
```

Su log samples

OpenBSD:

```
Feb 12 19:11:27 enigma su: dcid to root on /dev/ttyp0
Feb 12 19:11:41 enigma su: BAD SU dcid to root on /dev/ttyp0
Feb 12 19:11:48 enigma su: dcid to root on /dev/ttyp0
```

Solaris 10:

```
SU 07/23 00:57 + ??? root-root
SU 07/23 01:24 + pts/4 lcid-root
SU 07/23 19:12 + pts/2 lcid-root
SU 07/23 19:30 + pts/3 lcid-root
SU 07/23 19:32 - pts/3 lcid-root
SU 07/23 19:32 + pts/3 lcid-root
SU 02/12 19:27 + pts/2 lcid-root
SU 02/12 19:16 + pts/2 lcid-root
```

Slackware:

```
Jul  5 22:13:15 lili su[2614]: - pts/6 dcid-root
Jul  5 22:13:36 lili su[2711]: + pts/6 dcid-root
```

Ubuntu:

Messages from useradd, userdel, etc

Suse Linux useradd:

```
Sep 15 17:11:27 myserver useradd[13542]: new account added - account=fred, uid=1016, gid=100, home=/h
Sep 15 17:11:27 myserver useradd[13542]: account added to group - account=fred, group=video, gid=33,
Sep 15 17:11:27 myserver useradd[13542]: account added to group - account=fred, group=dialout, gid=16
Sep 15 17:11:27 myserver useradd[13542]: home directory created - account=fred, uid=1016, home=/home/
Sep 15 17:11:27 myserver useradd[13542]: running USERADD_CMD command - script=/usr/sbin/useradd.local
```

Suse Linux userdel:

```
Sep 15 16:37:13 myserver userdel[12584]: running USERDEL_PRECMD command - script=/usr/sbin/userdel-pr
Sep 15 16:37:13 myserver crontab[12586]: (root) DELETE (mary)
Sep 15 16:37:13 myserver userdel[12584]: account removed from group - account=mary, group=video, gid=
Sep 15 16:37:13 myserver userdel[12584]: account removed from group - account=mary, group=dialout, gi
Sep 15 16:37:13 myserver userdel[12584]: account deleted - account=mary, uid=1014, by=0
Sep 15 16:37:13 myserver userdel[12584]: running USERDEL_POSTCMD command - script=/usr/sbin/userdel-p
```

useradd&passwd fail:

```
May 28 16:04:10 server2 useradd[30245]: failed adding user 'avahi', data deleted
May 28 16:04:10 server2 passwd[30246]: password for 'avahi' changed by 'root'
May 28 16:04:12 server2 passwd[30263]: password for 'hal' changed by 'root'
May 28 16:07:10 server2 useradd[30523]: failed adding user 'mysql', data deleted
May 28 16:11:48 server2 passwd[32532]: password for 'gdm' changed by 'root'
May 28 16:16:07 server2 useradd[633]: failed adding user 'privoxy', data deleted
```

Linux Logs

Cron/Crontab Log Samples

Crontab edited by root:

```
Sep 11 09:46:33 sys1 crontab[20601]: (root) BEGIN EDIT (root)
Sep 11 09:46:39 sys1 crontab[20601]: (root) REPLACE (root)
Sep 11 09:46:39 sys1 crontab[20601]: (root) END EDIT (root)
```

This is root editing another user's crontab:

```
Sep 11 09:50:42 sys1 crontab[20230]: (root) BEGIN EDIT (user1)
Sep 11 09:51:06 sys1 crontab[20230]: (root) REPLACE (user1)
Sep 11 09:51:06 sys1 crontab[20230]: (root) END EDIT (user1)
```

This is a user editing their own crontab:

```
Sep 11 09:51:39 sys1 crontab[20761]: (user1) BEGIN EDIT (user1)
Sep 11 09:51:46 sys1 crontab[20761]: (user1) REPLACE (user1)
Sep 11 09:51:46 sys1 crontab[20761]: (user1) END EDIT (user1)
```

Additional samples:

```
Sep 11 15:20:57 copacabana crontab[7972]: (dcid) BEGIN EDIT (dcid)
Sep 11 15:21:26 copacabana crontab[7972]: (dcid) REPLACE (dcid)
Sep 11 15:21:26 copacabana crontab[7972]: (dcid) END EDIT (dcid)
Sep 11 15:22:01 copacabana /USR/SBIN/CRON[7993]: (dcid) CMD (/bin/xx)
Sep 11 15:22:01 copacabana /USR/SBIN/CRON[7992]: (dcid) MAIL (mailed 102 bytes of output but got stat
```

crond samples:

```
May 28 13:04:20 Lab7 crond[2843]: /usr/sbin/crond 4.4 dillon's cron daemon, started with loglevel not
May 28 13:04:20 Lab7 crond[2843]: no timestamp found (user root job sys-hourly)
May 28 13:04:20 Lab7 crond[2843]: no timestamp found (user root job sys-daily)
```

```
May 28 13:04:20 Lab7 crond[2843]: no timestamp found (user root job sys-weekly)
May 28 13:04:20 Lab7 crond[2843]: no timestamp found (user root job sys-monthly)
Jun 13 07:46:22 Lab7 crond[3592]: unable to exec /usr/sbin/sendmail: cron output for user root job sy
```

dpkg is the software at the base of the Debian package management system. dpkg is used to install, remove, and provide information about `.deb` packages.

```
2008-04-01 14:39:49 install screen <none> 4.0.3-0.3
2008-04-01 14:39:49 status half-installed screen 4.0.3-0.3
2008-04-01 14:39:51 status unpacked screen 4.0.3-0.3
2008-04-01 14:39:51 status unpacked screen 4.0.3-0.3
2008-04-01 14:39:51 status unpacked screen 4.0.3-0.3
2008-04-01 14:39:51 status unpacked screen 4.0.3-0.3
2008-04-01 14:39:51 status unpacked screen 4.0.3-0.3
2008-04-01 14:39:51 status half-configured screen 4.0.3-0.3
2008-04-01 14:39:54 status installed screen 4.0.3-0.3
2008-04-01 16:10:43 status installed nmap 4.11-1
2008-04-01 16:10:43 remove nmap 4.11-1 4.11-1
2008-04-01 16:10:43 status half-configured nmap 4.11-1
2008-04-01 16:10:43 status half-installed nmap 4.11-1
2008-04-01 16:10:43 status config-files nmap 4.11-1
2008-04-01 16:10:43 status config-files nmap 4.11-1
2008-04-01 16:10:43 status config-files nmap 4.11-1
2008-04-01 16:10:43 status not-installed nmap <none>
2008-04-01 16:10:56 install nmap <none> 4.11-1
2008-04-01 16:10:56 status half-installed nmap 4.11-1
2008-04-01 16:10:56 status unpacked nmap 4.11-1
2008-04-01 16:10:56 status unpacked nmap 4.11-1
2008-04-01 16:10:56 status unpacked nmap 4.11-1
2008-04-01 16:10:56 status half-configured nmap 4.11-1
2008-04-01 16:10:56 status installed nmap 4.11-1
2008-04-02 11:25:17 install mysql-common <none> 5.0.32-7etch5
2008-04-02 11:25:17 status half-installed mysql-common 5.0.32-7etch5
2008-04-02 11:25:17 status unpacked mysql-common 5.0.32-7etch5
2008-04-02 11:25:17 status unpacked mysql-common 5.0.32-7etch5
2008-04-02 11:25:17 install libnet-daemon-perl <none> 0.38-1.1
2008-04-02 11:25:17 status half-installed libnet-daemon-perl 0.38-1.1
2008-04-02 11:25:17 status unpacked libnet-daemon-perl 0.38-1.1
2008-04-02 11:25:17 status unpacked libnet-daemon-perl 0.38-1.1
2008-04-02 11:25:18 install libplrpc-perl <none> 0.2017-1.1
2008-04-02 11:25:18 status half-installed libplrpc-perl 0.2017-1.1
2008-04-02 11:25:18 status unpacked libplrpc-perl 0.2017-1.1
2008-04-02 11:25:18 status unpacked libplrpc-perl 0.2017-1.1
2008-04-02 11:25:18 install libdbi-perl <none> 1.53-1etch1
2008-04-02 11:25:18 status half-installed libdbi-perl 1.53-1etch1
2008-04-02 11:25:18 status unpacked libdbi-perl 1.53-1etch1
2008-04-02 11:25:18 status unpacked libdbi-perl 1.53-1etch1
2008-04-02 11:25:19 install libmysqlclient15off <none> 5.0.32-7etch5
2008-04-02 11:25:19 status half-installed libmysqlclient15off 5.0.32-7etch5
2008-04-02 11:25:19 status unpacked libmysqlclient15off 5.0.32-7etch5
2008-04-02 11:25:19 status unpacked libmysqlclient15off 5.0.32-7etch5
2008-04-02 11:25:19 install libdbd-mysql-perl <none> 3.0008-1
2008-04-02 11:25:19 status half-installed libdbd-mysql-perl 3.0008-1
2008-04-02 11:25:19 status unpacked libdbd-mysql-perl 3.0008-1
2008-04-02 11:25:19 status unpacked libdbd-mysql-perl 3.0008-1
2008-04-02 11:25:19 install mysql-client-5.0 <none> 5.0.32-7etch5
2008-04-02 11:25:19 status half-installed mysql-client-5.0 5.0.32-7etch5
2008-04-02 11:25:21 status unpacked mysql-client-5.0 5.0.32-7etch5
```

```
2008-04-02 11:25:21 status unpacked mysql-client-5.0 5.0.32-7etch5
2008-04-02 11:25:21 status unpacked mysql-common 5.0.32-7etch5
2008-04-02 11:25:21 status unpacked mysql-common 5.0.32-7etch5
2008-04-02 11:25:21 status half-configured mysql-common 5.0.32-7etch5
2008-04-02 11:25:21 status installed mysql-common 5.0.32-7etch5
2008-04-02 11:25:22 install mysql-server-5.0 <none> 5.0.32-7etch5
2008-04-02 11:25:22 status half-installed mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:35 status unpacked mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:36 status unpacked mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:36 install mysql-server <none> 5.0.32-7etch5
2008-04-02 11:25:36 status half-installed mysql-server 5.0.32-7etch5
2008-04-02 11:25:36 status unpacked mysql-server 5.0.32-7etch5
2008-04-02 11:25:36 status unpacked mysql-server 5.0.32-7etch5
2008-04-02 11:25:36 install php5-mysql <none> 5.2.0-8+etch10
2008-04-02 11:25:36 status half-installed php5-mysql 5.2.0-8+etch10
2008-04-02 11:25:36 status unpacked php5-mysql 5.2.0-8+etch10
2008-04-02 11:25:36 status unpacked php5-mysql 5.2.0-8+etch10
2008-04-02 11:25:36 install phpmyadmin <none> 4:2.9.1.1-6
2008-04-02 11:25:36 status half-installed phpmyadmin 4:2.9.1.1-6
2008-04-02 11:25:41 status unpacked phpmyadmin 4:2.9.1.1-6
2008-04-02 11:25:41 status unpacked phpmyadmin 4:2.9.1.1-6
2008-04-02 11:25:41 status unpacked libnet-daemon-perl 0.38-1.1
2008-04-02 11:25:41 status half-configured libnet-daemon-perl 0.38-1.1
2008-04-02 11:25:41 status installed libnet-daemon-perl 0.38-1.1
2008-04-02 11:25:41 status unpacked libplrpc-perl 0.2017-1.1
2008-04-02 11:25:41 status half-configured libplrpc-perl 0.2017-1.1
2008-04-02 11:25:41 status installed libplrpc-perl 0.2017-1.1
2008-04-02 11:25:41 status unpacked libdbi-perl 1.53-1etch1
2008-04-02 11:25:41 status half-configured libdbi-perl 1.53-1etch1
2008-04-02 11:25:41 status installed libdbi-perl 1.53-1etch1
2008-04-02 11:25:41 status unpacked libmysqlclient15off 5.0.32-7etch5
2008-04-02 11:25:41 status half-configured libmysqlclient15off 5.0.32-7etch5
2008-04-02 11:25:42 status installed libmysqlclient15off 5.0.32-7etch5
2008-04-02 11:25:42 status unpacked libdbd-mysql-perl 3.0008-1
2008-04-02 11:25:42 status half-configured libdbd-mysql-perl 3.0008-1
2008-04-02 11:25:42 status installed libdbd-mysql-perl 3.0008-1
2008-04-02 11:25:42 status unpacked mysql-client-5.0 5.0.32-7etch5
2008-04-02 11:25:42 status half-configured mysql-client-5.0 5.0.32-7etch5
2008-04-02 11:25:42 status installed mysql-client-5.0 5.0.32-7etch5
2008-04-02 11:25:42 status unpacked mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:42 status unpacked mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:42 status unpacked mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:42 status unpacked mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:42 status unpacked mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:42 status unpacked mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:42 status unpacked mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:42 status unpacked mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:42 status unpacked mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:42 status half-configured mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:59 status installed mysql-server-5.0 5.0.32-7etch5
2008-04-02 11:25:59 status unpacked mysql-server 5.0.32-7etch5
2008-04-02 11:25:59 status half-configured mysql-server 5.0.32-7etch5
2008-04-02 11:26:00 status installed mysql-server 5.0.32-7etch5
2008-04-02 11:26:00 status unpacked php5-mysql 5.2.0-8+etch10
2008-04-02 11:26:00 status unpacked php5-mysql 5.2.0-8+etch10
2008-04-02 11:26:00 status unpacked php5-mysql 5.2.0-8+etch10
2008-04-02 11:26:00 status unpacked php5-mysql 5.2.0-8+etch10
2008-04-02 11:26:00 status half-configured php5-mysql 5.2.0-8+etch10
```

```
2008-04-02 11:26:00 status installed php5-mysql 5.2.0-8+etch10
2008-04-02 11:26:00 status unpacked phpmyadmin 4:2.9.1.1-6
2008-04-02 11:26:00 status half-configured phpmyadmin 4:2.9.1.1-6
2008-04-02 11:26:15 status installed phpmyadmin 4:2.9.1.1-6
2008-04-02 13:45:39 install zlib1g-dev <none> 1:1.2.3-13
2008-04-02 13:45:39 status half-installed zlib1g-dev 1:1.2.3-13
2008-04-02 13:45:39 status unpacked zlib1g-dev 1:1.2.3-13
2008-04-02 13:45:40 status unpacked zlib1g-dev 1:1.2.3-13
2008-04-02 13:45:40 install libmysqlclient15-dev <none> 5.0.32-7etch5
2008-04-02 13:45:40 status half-installed libmysqlclient15-dev 5.0.32-7etch5
2008-04-02 13:45:41 status unpacked libmysqlclient15-dev 5.0.32-7etch5
2008-04-02 13:45:41 status unpacked libmysqlclient15-dev 5.0.32-7etch5
2008-04-02 13:45:42 status unpacked zlib1g-dev 1:1.2.3-13
2008-04-02 13:45:42 status half-configured zlib1g-dev 1:1.2.3-13
2008-04-02 13:45:42 status installed zlib1g-dev 1:1.2.3-13
2008-04-02 13:45:42 status unpacked libmysqlclient15-dev 5.0.32-7etch5
2008-04-02 13:45:42 status half-configured libmysqlclient15-dev 5.0.32-7etch5
2008-04-02 13:45:42 status installed libmysqlclient15-dev 5.0.32-7etch5
2008-04-03 14:03:54 install proftpd <none> 1.3.0-19
2008-04-03 14:03:54 status half-installed proftpd 1.3.0-19
2008-04-03 14:03:55 status unpacked proftpd 1.3.0-19
2008-04-03 14:03:55 status unpacked proftpd 1.3.0-19
2008-04-03 14:03:55 status unpacked proftpd 1.3.0-19
2008-04-03 14:03:55 status unpacked proftpd 1.3.0-19
2008-04-03 14:03:55 status unpacked proftpd 1.3.0-19
2008-04-03 14:03:55 status unpacked proftpd 1.3.0-19
2008-04-03 14:03:55 status unpacked proftpd 1.3.0-19
2008-04-03 14:03:55 status unpacked proftpd 1.3.0-19
2008-04-03 14:03:55 status half-configured proftpd 1.3.0-19
2008-04-03 14:04:01 status installed proftpd 1.3.0-19
2008-04-03 14:47:27 status installed klogd 1.4.1-18
2008-04-03 14:47:27 status installed sysklogd 1.4.1-18
2008-04-03 14:47:27 status installed klogd 1.4.1-18
2008-04-03 14:47:27 status installed sysklogd 1.4.1-18
2008-04-03 14:47:27 status installed klogd 1.4.1-18
2008-04-03 14:47:27 status installed sysklogd 1.4.1-18
2008-04-03 14:47:27 status installed klogd 1.4.1-18
2008-04-03 14:47:27 status installed sysklogd 1.4.1-18
2008-04-03 14:47:27 status installed klogd 1.4.1-18
2008-04-03 14:47:27 status installed sysklogd 1.4.1-18
2008-04-03 14:47:27 status installed klogd 1.4.1-18
2008-04-03 14:47:28 remove klogd 1.4.1-18 1.4.1-18
2008-04-03 14:47:28 status half-configured klogd 1.4.1-18
2008-04-03 14:47:28 status half-installed klogd 1.4.1-18
2008-04-03 14:47:28 status config-files klogd 1.4.1-18
2008-04-03 14:47:28 status config-files klogd 1.4.1-18
2008-04-03 14:47:28 status installed sysklogd 1.4.1-18
2008-04-03 14:47:28 remove sysklogd 1.4.1-18 1.4.1-18
2008-04-03 14:47:28 status half-configured sysklogd 1.4.1-18
2008-04-03 14:47:29 status half-installed sysklogd 1.4.1-18
2008-04-03 14:47:29 status config-files sysklogd 1.4.1-18
2008-04-03 14:47:29 status config-files sysklogd 1.4.1-18
2008-04-03 14:47:29 install syslog-ng <none> 2.0.0-1etch1
2008-04-03 14:47:29 status half-installed syslog-ng 2.0.0-1etch1
2008-04-03 14:47:30 status unpacked syslog-ng 2.0.0-1etch1
2008-04-03 14:47:30 status unpacked syslog-ng 2.0.0-1etch1
```

```
2008-04-03 14:47:30 status unpacked syslog-ng 2.0.0-1etch1
2008-04-03 14:47:30 status unpacked syslog-ng 2.0.0-1etch1
2008-04-03 14:47:30 status unpacked syslog-ng 2.0.0-1etch1
2008-04-03 14:47:30 status unpacked syslog-ng 2.0.0-1etch1
2008-04-03 14:47:30 status unpacked syslog-ng 2.0.0-1etch1
2008-04-03 14:47:30 status unpacked syslog-ng 2.0.0-1etch1
2008-04-03 14:47:30 status unpacked syslog-ng 2.0.0-1etch1
2008-04-03 14:47:30 status unpacked syslog-ng 2.0.0-1etch1
2008-04-03 14:47:30 status half-configured syslog-ng 2.0.0-1etch1
2008-04-03 14:47:31 status installed syslog-ng 2.0.0-1etch1
2008-04-03 14:48:36 status config-files sysklogd 1.4.1-18
2008-04-03 14:48:36 remove sysklogd 1.4.1-18 1.4.1-18
2008-04-03 14:48:36 purge sysklogd 1.4.1-18 1.4.1-18
2008-04-03 14:48:36 status config-files sysklogd 1.4.1-18
2008-04-03 14:48:36 status config-files sysklogd 1.4.1-18
2008-04-03 14:48:36 status config-files sysklogd 1.4.1-18
2008-04-03 14:48:36 status config-files sysklogd 1.4.1-18
2008-04-03 14:48:36 status config-files sysklogd 1.4.1-18
2008-04-03 14:48:36 status not-installed sysklogd <none>
2008-04-03 14:50:03 status installed syslog-ng 2.0.0-1etch1
2008-04-03 14:50:04 remove syslog-ng 2.0.0-1etch1 2.0.0-1etch1
2008-04-03 14:50:04 status half-configured syslog-ng 2.0.0-1etch1
2008-04-03 14:50:04 status half-installed syslog-ng 2.0.0-1etch1
2008-04-03 14:50:04 status config-files syslog-ng 2.0.0-1etch1
2008-04-03 14:50:04 status config-files syslog-ng 2.0.0-1etch1
2008-04-03 14:50:10 status config-files syslog-ng 2.0.0-1etch1
2008-04-03 14:50:10 remove syslog-ng 2.0.0-1etch1 2.0.0-1etch1
2008-04-03 14:50:10 purge syslog-ng 2.0.0-1etch1 2.0.0-1etch1
2008-04-03 14:50:10 status config-files syslog-ng 2.0.0-1etch1
2008-04-03 14:50:10 status config-files syslog-ng 2.0.0-1etch1
2008-04-03 14:50:10 status config-files syslog-ng 2.0.0-1etch1
2008-04-03 14:50:10 status config-files syslog-ng 2.0.0-1etch1
2008-04-03 14:50:10 status config-files syslog-ng 2.0.0-1etch1
2008-04-03 14:50:11 status not-installed syslog-ng <none>
2008-04-03 14:50:22 install sysklogd <none> 1.4.1-18
2008-04-03 14:50:22 status half-installed sysklogd 1.4.1-18
2008-04-03 14:50:22 status unpacked sysklogd 1.4.1-18
2008-04-03 14:50:22 status unpacked sysklogd 1.4.1-18
2008-04-03 14:50:22 install klogd 1.4.1-18 1.4.1-18
2008-04-03 14:50:22 status half-installed klogd 1.4.1-18
2008-04-03 14:50:22 status unpacked klogd 1.4.1-18
2008-04-03 14:50:22 status unpacked klogd 1.4.1-18
2008-04-03 14:50:23 status unpacked sysklogd 1.4.1-18
2008-04-03 14:50:23 status unpacked sysklogd 1.4.1-18
2008-04-03 14:50:23 status unpacked sysklogd 1.4.1-18
2008-04-03 14:50:23 status unpacked sysklogd 1.4.1-18
2008-04-03 14:50:23 status unpacked sysklogd 1.4.1-18
2008-04-03 14:50:23 status unpacked sysklogd 1.4.1-18
2008-04-03 14:50:23 status half-configured sysklogd 1.4.1-18
2008-04-03 14:50:24 status installed sysklogd 1.4.1-18
2008-04-03 14:50:24 status unpacked klogd 1.4.1-18
2008-04-03 14:50:24 status unpacked klogd 1.4.1-18
2008-04-03 14:50:24 status unpacked klogd 1.4.1-18
2008-04-03 14:50:24 status half-configured klogd 1.4.1-18
2008-04-03 14:50:24 status installed klogd 1.4.1-18
```

Log Samples from the Linux kernel

NFS incompability between Linux and Solaris (not security related):

```
Feb 28 07:46:15 bs11 kernel: svc: unknown program 100227 (me 100003)
```

System shutdown:

```
Jun  1 22:20:05 secserv kernel: Kernel logging (proc) stopped.
Jun  1 22:20:05 secserv kernel: Kernel log daemon terminating.
Jun  1 22:20:06 secserv exiting on signal 15
Nov 27 08:05:57 galileo kernel: Kernel logging (proc) stopped.
Nov 27 08:05:57 galileo kernel: Kernel log daemon terminating.
Nov 27 08:05:57 galileo exiting on signal 15
```

ADSL monitor:

```
Nov 22 02:35:36 thecla2 kernel: ATM dev 0: ADSL line is up (2752 kb/s down | 448 kb/s up)
```

description:

```
May 21 20:22:28 slacker2 kernel: tcp_parse_options: Illegal window scaling value 200 >14 received.
```

Kernel level hardware SCSI error (not security related):

```
Aug 30 10:06:11 newfish kernel: >>>>>>>>>>>>>>>>>> Dump Card State Begins <<<<<<<<<<<<<<<<<
Aug 30 10:06:11 newfish kernel: scsi1: Dumping Card State in Message-out phase, at SEQADDR 0x16b
Aug 30 10:06:11 newfish kernel: Card was paused
Aug 30 10:06:11 newfish kernel: ACCUM = 0xa0, SINDEX = 0x61, DINDEX = 0xe4, ARG_2 = 0x1
Aug 30 10:06:11 newfish kernel: HCNT = 0x0 SCBPTR = 0x1
Aug 30 10:06:11 newfish kernel: SCSIPHASE[0x0] SCSISIGI[0xa4] ERROR[0x0] SCSIBUSL[0xd]
Aug 30 10:06:11 newfish kernel: LASTPHASE[0xa0] SCSISEQ[0x12] SBLKCTL[0xa] SCSIRATE[0xc2]
Aug 30 10:06:11 newfish kernel: SEQCTL[0x10] SEQ_FLAGS[0x40] SSTAT0[0x0] SSTAT1[0x0]
Aug 30 10:06:11 newfish kernel: SSTAT2[0x0] SSTAT3[0x0] SIMODE0[0x8] SIMODE1[0xac]
Aug 30 10:06:11 newfish kernel: SXFRCTL0[0x88] DFCNTRL[0x0] DFSTATUS[0x89]
Aug 30 10:06:11 newfish kernel: STACK: 0xe1 0xe1 0x163 0x178
Aug 30 10:06:11 newfish kernel: SCB count = 12
Aug 30 10:06:11 newfish kernel: Kernel NEXTQSCB = 11
Aug 30 10:06:11 newfish kernel: Card NEXTQSCB = 4
Aug 30 10:06:12 newfish kernel: QINFIFO entries: 4
Aug 30 10:06:12 newfish kernel: Waiting Queue entries:
Aug 30 10:06:12 newfish kernel: Disconnected Queue entries: 2:7
Aug 30 10:06:12 newfish kernel: QOUTFIFO entries:
Aug 30 10:06:12 newfish kernel: Sequencer Free SCB List: 0 6 7 5 4 3 8 9 10 11 12 13 14 15 16 17 18 1
Aug 30 10:06:12 newfish kernel: Sequencer SCB Info:
Aug 30 10:06:12 newfish kernel:   0 SCB_CONTROL[0x0] SCB_SCSIID[0x17] SCB_LUN[0x0] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:   1 SCB_CONTROL[0x64] SCB_SCSIID[0x17] SCB_LUN[0x0] SCB_TAG[0x5]
Aug 30 10:06:12 newfish kernel:   2 SCB_CONTROL[0x64] SCB_SCSIID[0x17] SCB_LUN[0x0] SCB_TAG[0x7]
Aug 30 10:06:12 newfish kernel:   3 SCB_CONTROL[0xe0] SCB_SCSIID[0x7] SCB_LUN[0x0] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:   4 SCB_CONTROL[0xe0] SCB_SCSIID[0x7] SCB_LUN[0x0] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:   5 SCB_CONTROL[0xe0] SCB_SCSIID[0x17] SCB_LUN[0x0] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:   6 SCB_CONTROL[0x0] SCB_SCSIID[0x17] SCB_LUN[0x0] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:   7 SCB_CONTROL[0xe0] SCB_SCSIID[0x17] SCB_LUN[0x0] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:   8 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:   9 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:  10 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:  11 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
```

```
Aug 30 10:06:12 newfish kernel:  12 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:  13 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:  14 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:  15 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:  16 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:  17 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:12 newfish kernel:  18 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  19 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  20 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  21 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  22 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  23 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  24 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  25 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  26 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  27 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  28 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  29 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  30 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel:  31 SCB_CONTROL[0x0] SCB_SCSIID[0xff] SCB_LUN[0xff] SCB_TAG[0xff]
Aug 30 10:06:13 newfish kernel: Pending list:
Aug 30 10:06:13 newfish kernel:   7 SCB_CONTROL[0x60] SCB_SCSIID[0x17] SCB_LUN[0x0]
Aug 30 10:06:13 newfish kernel:   4 SCB_CONTROL[0x74] SCB_SCSIID[0x17] SCB_LUN[0x0]
Aug 30 10:06:13 newfish kernel:   5 SCB_CONTROL[0x64] SCB_SCSIID[0x17] SCB_LUN[0x0]
Aug 30 10:06:13 newfish kernel: Kernel Free SCB list: 1 0 2 3 6 10 9 8
Aug 30 10:06:13 newfish kernel: DevQ(0:0:0): 0 waiting
Aug 30 10:06:13 newfish kernel: DevQ(0:1:0): 0 waiting
Aug 30 10:06:13 newfish kernel: DevQ(0:6:0): 0 waiting
Aug 30 10:06:13 newfish kernel:
Aug 30 10:06:13 newfish kernel: <<<<<<<<<<<<<<<< Dump Card State Ends >>>>>>>>>>>>>>>>>>
Aug 30 10:06:13 newfish kernel: Recovery SCB completes
Aug 30 10:06:13 newfish kernel: (scsi1:A:1:0): Device is disconnected, re-queuing SCB
Aug 30 10:06:13 newfish kernel: Recovery code sleeping
Aug 30 10:06:13 newfish kernel: Recovery code awake
Aug 30 10:06:13 newfish kernel: Timer Expired
Aug 30 10:06:13 newfish kernel: aic7xxx_abort returns 0x2003
Aug 30 10:06:13 newfish kernel: scsi1:0:1:0: Attempting to queue a TARGET RESET message
Aug 30 10:06:13 newfish kernel: CDB: 0x28 0x0 0x4 0x7a 0x65 0xcf 0x0 0x0 0x10 0x0
Aug 30 10:06:13 newfish kernel: aic7xxx_dev_reset returns 0x2003
Aug 30 10:06:13 newfish kernel: Recovery SCB completes
```

Linux BUG and call trace example:

```
BUG: unable to handle kernel NULL pointer dereference at (null)
IP: [<ffffffff8141c423>] 0xffffffff8141c423
PGD 0
Oops: 0002 [#1] PREEMPT SMP
last sysfs file: /sys/devices/pci0000:00/0000:00:1f.2/host0/target0:0:0/0:0:0:0/scsi_level
CPU 0
Modules linked in: zr364xx videodev v4l1_compat v4l2_compat_ioctl32 videobuf_vmalloc videobuf_core us
ieee80211_rtl ieee80211_crypt_ccmp_rtl ieee80211_crypt_tkip_rtl ieee80211_crypt_wep_rtl ieee80211_cry
snd_seq_dummy sdhci_pci sdhci snd_seq_oss snd_hda_codec_realtek snd_seq_midi_event snd_seq snd_seq_de
mmc_core iTCO_wdt iTCO_vendor_support nvidia(P) snd_hda_intel snd_hda_codec snd_hwdep snd_pcm_oss snd
snd_timer snd_page_alloc snd_mixer_oss snd soundcore r8169 mii pata_acpi [last unloaded: ieee80211_cr
Pid: 226, comm: khubd Tainted: P           2.6.30.5 #1 GX700
RIP: 0010:[<ffffffff8141c423>]  [<ffffffff8141c423>] 0xffffffff8141c423
RSP: 0018:ffff8800bfa2fc08  EFLAGS: 00010246
RAX: 0000000000000000 RBX: ffff8800b0953d14 RCX: 0000000000000000
```

```
RDX: 0000000000000000 RSI: 0000000000000083 RDI: ffff8800b0953d14
RBP: ffff8800b0953d10 R08: 0000000000000000 R09: 00000000000000ae
R10: ffff880001744540 R11: 0000000000000008 R12: ffffffffffffffff
R13: ffff8800b0953d18 R14: 0000000000000000 R15: ffff8800bf8671c0
FS:  0000000000000000(0000) GS:ffff88000165f000(0000) knlGS:0000000000000000
CS:  0010 DS: 0018 ES: 0018 CR0: 000000008005003b
CR2: 0000000000000000 CR3: 0000000001001000 CR4: 00000000000006e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7: 0000000000000400
Process khubd (pid: 226, threadinfo ffff8800bfa2e000, task ffff8800bf8671c0)
Stack:
 ffff8800b0953d18 ffff8800a9049c30 ffff8800bfa2fc60 ffff8800bfa2fcb0
 ffffffff8110aaaa ffff8800b0953d10 ffff8800b08a5c00 ffffffffa09ea788
 ffff8800bb05f800 000000000000001f 0000000000000000 ffffffff8141c06a
Call Trace:
 [<ffffffff8110aaaa>] ? 0xffffffff8110aaaa
 [<ffffffff8141c06a>] ? 0xffffffff8141c06a
 [<ffffffffa09cd5e6>] ? 0xffffffffa09cd5e6
 [<ffffffffa09e711a>] ? 0xffffffffa09e711a
 [<ffffffff812a8878>] ? 0xffffffff812a8878
 [<ffffffff81246932>] ? 0xffffffff81246932
 [<ffffffff81246a55>] ? 0xffffffff81246a55
 [<ffffffff81245bf1>] ? 0xffffffff81245bf1
 [<ffffffff81244208>] ? 0xffffffff81244208
 [<ffffffff812a609a>] ? 0xffffffff812a609a
 [<ffffffff812a12b9>] ? 0xffffffff812a12b9
 [<ffffffff812a214f>] ? 0xffffffff812a214f
 [<ffffffff810098cc>] ? 0xffffffff810098cc
 [<ffffffff81033551>] ? 0xffffffff81033551
 [<ffffffff8141dc39>] ? 0xffffffff8141dc39
 [<ffffffff81053f10>] ? 0xffffffff81053f10
 [<ffffffff812a1cf0>] ? 0xffffffff812a1cf0
 [<ffffffff81053b24>] ? 0xffffffff81053b24
 [<ffffffff8100c57a>] ? 0xffffffff8100c57a
 [<ffffffff81053ad0>] ? 0xffffffff81053ad0
 [<ffffffff8100c570>] ? 0xffffffff8100c570
Code: 7f b6 66 0f 1f 44 00 00 48 8d 5d 04 4c 8d 6d 08 48 89 df 49 c7 c4 ff ff ff ff e8 c9 14 00 00 48
RIP  [<ffffffff8141c423>] 0xffffffff8141c423
 RSP <ffff8800bfa2fc08>
CR2: 0000000000000000
---[ end trace 05e0b9e1e8d124aa ]---
note: khubd[226] exited with preempt_count 2
```

SLUB mem allocate failed(swapper: page allocation failure.)

```
Feb 20 21:20:06 server1 kernel: SLUB: Unable to allocate memory on node -1 (gfp=0x20)
Feb 20 21:20:06 server1 kernel:  cache: kmalloc-4096, object size: 4096, buffer size: 4096, default o
Feb 20 21:20:06 server1 kernel:  node 0: slabs: 619, objs: 1641, free: 0
Feb 20 21:20:06 server1 kernel: swapper: page allocation failure. order:0, mode:0x4020
Feb 20 21:20:06 server1 kernel: Pid: 0, comm: swapper Not tainted 2.6.32.4 #1
Feb 20 21:20:06 server1 kernel: Call Trace:
Feb 20 21:20:06 server1 kernel: <IRQ>  [<ffffffff81084d3a>] ? __alloc_pages_nodemask+0x54a/0x670
Feb 20 21:20:06 server1 kernel: [<ffffffff810b1f8a>] ? __slab_alloc+0x69a/0x6b0
Feb 20 21:20:06 server1 kernel: [<ffffffff81710ee7>] ? __netdev_alloc_skb+0x17/0x40
Feb 20 21:20:06 server1 kernel: [<ffffffff8178309d>] ? tcp_v4_rcv+0x6bd/0x780
Feb 20 21:20:06 server1 kernel: [<ffffffff81710ee7>] ? __netdev_alloc_skb+0x17/0x40
Feb 20 21:20:06 server1 kernel: [<ffffffff810b2f0b>] ? __kmalloc_track_caller+0xcb/0x110
Feb 20 21:20:06 server1 kernel: [<ffffffff81710b6b>] ? __alloc_skb+0x6b/0x170
```

```
Feb 20 21:20:06 server1 kernel: [<ffffffff81710ee7>] ? __netdev_alloc_skb+0x17/0x40
Feb 20 21:20:06 server1 kernel: [<ffffffff8164fa29>] ? rtl8169_rx_fill+0xc9/0x220
Feb 20 21:20:06 server1 kernel: [<ffffffff8164fdc0>] ? rtl8169_rx_interrupt+0x240/0x520
Feb 20 21:20:06 server1 kernel: [<ffffffff81650236>] ? rtl8169_poll+0x56/0x240
Feb 20 21:20:06 server1 kernel: [<ffffffff8171d513>] ? net_rx_action+0x83/0x130
Feb 20 21:20:06 server1 kernel: [<ffffffff81049dd6>] ? __do_softirq+0xa6/0x130
Feb 20 21:20:06 server1 kernel: [<ffffffff8100c5ec>] ? call_softirq+0x1c/0x30
Feb 20 21:20:06 server1 kernel: [<ffffffff8100e58d>] ? do_softirq+0x4d/0x80
Feb 20 21:20:06 server1 kernel: [<ffffffff81049c15>] ? irq_exit+0x95/0xa0
Feb 20 21:20:06 server1 kernel: [<ffffffff8100db8e>] ? do_IRQ+0x6e/0xe0
Feb 20 21:20:06 server1 kernel: [<ffffffff8100be53>] ? ret_from_intr+0x0/0xa
Feb 20 21:20:06 server1 kernel: <EOI>  [<ffffffff8101f020>] ? lapic_next_event+0x0/0x20
Feb 20 21:20:06 server1 kernel: [<ffffffff81013452>] ? default_idle+0x32/0x40
Feb 20 21:20:06 server1 kernel: [<ffffffff81013494>] ? c1e_idle+0x34/0x100
Feb 20 21:20:06 server1 kernel: [<ffffffff8100a14c>] ? cpu_idle+0xac/0x100
```

example segfault log

```
Jun 20 09:44:14 srv1 kernel: chttp[5849] general protection ip:7f185c076c93 sp:7fff38b79610 error:0 i
Jun 20 09:56:31 srv1 kernel: chttp[5883]: segfault at 0 ip 00007f0cc4898af0 sp 00007fff0b43d5f8 erro
```

cdrom errors:

```
Jun  7 15:32:50 Lab4 kernel: cdrom: This disc doesn't have any tracks I recognize!
Jun  7 15:32:50 Lab4 kernel: sr 3:0:0:0: [sr0] Result: hostbyte=DID_OK driverbyte=DRIVER_SENSE
Jun  7 15:32:50 Lab4 kernel: sr 3:0:0:0: [sr0] Sense Key : Illegal Request [current]
Jun  7 15:32:50 Lab4 kernel: Info fld=0x0
Jun  7 15:32:50 Lab4 kernel: sr 3:0:0:0: [sr0] Add. Sense: Logical block address out of range
Jun  7 15:32:50 Lab4 kernel: sr 3:0:0:0: [sr0] CDB: Read(10): 28 00 00 00 00 00 00 00 01 00
Jun  7 15:32:50 Lab4 kernel: end_request: I/O error, dev sr0, sector 0
Jun  7 15:32:50 Lab4 kernel: Buffer I/O error on device sr0, logical block 0
```

USB flash drive connect: Maybe use this to block if someone plugs in an usb stick and rip some data from the server.

```
Jun 27 16:42:52 Lab14 kernel: usb 3-1.2: new full speed USB device using uhci_hcd and address 6
Jun 27 16:42:52 Lab14 kernel: usb 3-1.2: not running at top speed; connect to a high speed hub
Jun 27 16:42:52 Lab14 kernel: scsi5 : usb-storage 3-1.2:1.0
Jun 27 16:42:53 Lab14 kernel: scsi 5:0:0:0: Direct-Access     Ut165    USB2FlashStorage 0.00 PQ: 0 AN
Jun 27 16:42:53 Lab14 kernel: sd 5:0:0:0: Attached scsi generic sg2 type 0
Jun 27 16:42:53 Lab14 kernel: sd 5:0:0:0: [sdb] 15794176 512-byte logical blocks: (8.08 GB/7.53 GiB)
Jun 27 16:42:53 Lab14 kernel: sd 5:0:0:0: [sdb] Write Protect is off
Jun 27 16:42:53 Lab14 kernel: sdb: unknown partition table
Jun 27 16:42:53 Lab14 kernel: sd 5:0:0:0: [sdb] Attached SCSI removable disk
Jun 27 16:43:01 Lab14 kernel: EXT3-fs: barriers not enabled
Jun 27 16:43:01 Lab14 kernel: kjournald starting.  Commit interval 5 seconds
Jun 27 16:43:01 Lab14 kernel: EXT3-fs (sdb): warning: maximal mount count reached, running e2fsck is
Jun 27 16:43:01 Lab14 kernel: EXT3-fs (sdb): using internal journal
Jun 27 16:43:01 Lab14 kernel: EXT3-fs (sdb): mounted filesystem with writeback data mode
```

Log Samples from pacman

pacman install log

```
[2010-05-28 14:41] installed filesystem (2010.02-4)
[2010-05-28 14:41] installed util-linux-ng (2.17.2-2)
[2010-05-28 14:41] installed e2fsprogs (1.41.11-1)
[2010-05-28 14:41] installed cryptsetup (1.1.0-2)
[2010-05-28 14:41] installed dash (0.5.5.1-2)
[2010-05-28 14:41] installed dcron (4.4-2)
[2010-05-28 14:41] installed dhcpcd (5.2.2-1)
[2010-05-28 14:41] installed diffutils (3.0-1)
[2010-05-28 14:41] installed file (5.04-2)
[2010-05-28 14:41] installed findutils (4.4.2-2)
[2010-05-28 14:41] installed gawk (3.1.8-1)
[2010-05-28 14:41] installed gen-init-cpio (2.6.32-1)
[2010-05-28 14:41] installed gettext (0.17-4)
[2010-05-28 14:41] installed pcre (8.02-1)
[2010-05-28 14:41] installed grep (2.6.3-1)
[2010-05-28 14:41] installed sed (4.2.1-2)
[2010-05-28 14:41] installed grub (0.97-17)
[2010-05-28 14:41] installed gzip (1.4-1)
[2010-05-28 14:41] installed libusb (0.1.12-4)
[2010-05-28 14:41] installed glib2 (2.24.1-1)
[2010-05-28 14:41] installed module-init-tools (3.11.1-2)
[2010-05-28 14:41] installed udev (151-3)
[2010-05-28 14:41] installed net-tools (1.60-14)
[2010-05-28 14:41] installed kbd (1.15.2-1)
[2010-05-28 14:41] installed sysvinit (2.86-5)
[2010-05-28 14:41] installed initscripts (2010.05-3)
[2010-05-28 14:41] installed iputils (20100214-2)
[2010-05-28 14:41] installed jfsutils (1.1.14-1)
[2010-05-28 14:41] installed kernel26-firmware (2.6.33.4-1)
[2010-05-28 14:41] installed mkinitcpio-busybox (1.16.1-3)
[2010-05-28 14:41] installed which (2.20-3)
[2010-05-28 14:41] installed mkinitcpio (0.6.4-1)
[2010-05-28 12:41] >>> Updating module dependencies. Please wait ...
[2010-05-28 12:41] >>> MKINITCPIO SETUP
[2010-05-28 12:41] >>> ----------------
[2010-05-28 12:41] >>> If you use LVM2, Encrypted root or software RAID,
[2010-05-28 12:41] >>> Ensure you enable support in /etc/mkinitcpio.conf .
[2010-05-28 12:41] >>> More information about mkinitcpio setup can be found here:
[2010-05-28 12:41] >>> http://wiki.archlinux.org/index.php/Mkinitcpio
[2010-05-28 12:41]
[2010-05-28 12:41] >>> Generating initial ramdisk, using mkinitcpio.  Please wait...
[2010-05-28 12:41] > Building image "default"
[2010-05-28 12:41] > Running command: /sbin/mkinitcpio -k 2.6.33-ARCH -c /etc/mkinitcpio.conf -g /boo
[2010-05-28 12:41] :: Begin build
[2010-05-28 12:41] :: Parsing hook [base]
[2010-05-28 12:41] :: Parsing hook [udev]
[2010-05-28 12:41] :: Parsing hook [autodetect]
[2010-05-28 12:41] :: Parsing hook [pata]
[2010-05-28 12:41] :: Parsing hook [scsi]
[2010-05-28 12:41] :: Parsing hook [sata]
[2010-05-28 12:41] :: Parsing hook [filesystems]
[2010-05-28 12:41] :: Generating module dependencies
[2010-05-28 12:41] :: Generating image '/boot/kernel26.img'...SUCCESS
[2010-05-28 12:41] > SUCCESS
[2010-05-28 12:41] > Building image "fallback"
[2010-05-28 12:41] > Running command: /sbin/mkinitcpio -k 2.6.33-ARCH -c /etc/mkinitcpio.conf -g /boo
[2010-05-28 12:41] :: Begin build
[2010-05-28 12:41] :: Parsing hook [base]
```

```
[2010-05-28 12:41] :: Parsing hook [udev]
[2010-05-28 12:41] :: Parsing hook [pata]
[2010-05-28 12:41] :: Parsing hook [scsi]
[2010-05-28 12:41] :: Parsing hook [sata]
[2010-05-28 12:41] :: Parsing hook [filesystems]
[2010-05-28 12:41] :: Generating module dependencies
[2010-05-28 12:41] :: Generating image '/boot/kernel26-fallback.img'...SUCCESS
[2010-05-28 12:41] > SUCCESS
[2010-05-28 14:41] installed kernel26 (2.6.33.4-1)
[2010-05-28 14:41] installed less (436-1)
[2010-05-28 14:41] installed licenses (2.6-1)
[2010-05-28 14:41] installed logrotate (3.7.8-1)
[2010-05-28 14:41] installed lvm2 (2.02.62-1)
[2010-05-28 14:41] installed lzo2 (2.03-1)
[2010-05-28 14:41] installed mailx (8.1.1-7)
[2010-05-28 14:41] installed gdbm (1.8.3-7)
[2010-05-28 14:41] installed perl (5.10.1-5)
[2010-05-28 14:42] installed texinfo (4.13a-4)
[2010-05-28 14:42] installed groff (1.20.1-4)
[2010-05-28 12:42] it's recommended to create an initial
[2010-05-28 12:42] database running as root:
[2010-05-28 12:42] "/usr/bin/mandb --quiet"
[2010-05-28 14:42] installed man-db (2.5.7-1)
[2010-05-28 14:42] installed man-pages (3.24-1)
[2010-05-28 14:42] installed mdadm (3.1.2-2)
[2010-05-28 14:42] installed nano (2.2.4-1)
[2010-05-28 14:42] installed xz-utils (4.999.9beta-2)
[2010-05-28 14:42] installed openssl (1.0.0-2)
[2010-05-28 14:42] installed expat (2.0.1-5)
[2010-05-28 14:42] installed libarchive (2.8.3-3)
[2010-05-28 14:42] installed libfetch (2.30-3)
[2010-05-28 14:42] installed pacman-mirrorlist (20100131-1)
[2010-05-28 14:42] installed pacman (3.3.3-5)
[2010-05-28 14:42] installed pciutils (3.1.7-1)
[2010-05-28 14:42] installed sysfsutils (2.1.0-5)
[2010-05-28 14:42] installed pcmciautils (016-1)
[2010-05-28 14:42] installed libnl (1.1-2)
[2010-05-28 14:42] installed libpcap (1.1.1-1)
[2010-05-28 14:42] installed ppp (2.4.5-1)
[2010-05-28 14:42] installed procps (3.2.8-1)
[2010-05-28 14:42] installed psmisc (22.11-1)
[2010-05-28 14:42] installed reiserfsprogs (3.6.21-2)
[2010-05-28 12:42] >>> The kernel-mode plugin has a new place.
[2010-05-28 12:42] >>> It's now located under /usr/lib/rp-pppoe/rp-pppoe.so
[2010-05-28 12:42] >>> Change LINUX_PLUGIN to the new path in your /etc/ppp/pppoe.conf
[2010-05-28 14:42] installed rp-pppoe (3.10-5)
[2010-05-28 14:42] installed eventlog (0.2.9-1)
[2010-05-28 14:42] installed tcp_wrappers (7.6-11)
[2010-05-28 14:42] installed syslog-ng (3.1.0-1)
[2010-05-28 14:42] installed tar (1.23-1)
[2010-05-28 14:42] installed usbutils (0.87-1)
[2010-05-28 14:42] installed vi (050325-3)
[2010-05-28 14:42] installed wget (1.12-2)
[2010-05-28 14:42] installed dbus-core (1.2.24-1)
[2010-05-28 14:42] installed wpa_supplicant (0.6.10-2)
[2010-05-28 14:42] installed xfsprogs (3.1.1-1)
[2010-05-28 14:42] installed m4 (1.4.14-1)
[2010-05-28 14:42] installed autoconf (2.65-2)
```

```
[2010-05-28 14:42] installed automake (1.11.1-1)
[2010-05-28 14:42] installed bin86 (0.16.17-4)
[2010-05-28 14:42] installed bison (2.4.2-1)
[2010-05-28 14:42] installed ed (1.4-2)
[2010-05-28 14:42] installed fakeroot (1.14.4-2)
[2010-05-28 14:42] installed flex (2.5.35-3)
[2010-05-28 14:42] installed mpfr (2.4.2-2)
[2010-05-28 14:42] installed libmpc (0.8.1-2)
[2010-05-28 14:42] installed ppl (0.10.2-3)
[2010-05-28 14:42] installed cloog-ppl (0.15.9-1)
[2010-05-28 14:42] installed libelf (0.8.13-1)
[2010-05-28 14:42] installed gcc (4.5.0-1)
[2010-05-28 14:42] installed libtool (2.2.6b-3)
[2010-05-28 14:42] installed make (3.81-5)
[2010-05-28 14:42] installed patch (2.6.1-1)
[2010-05-28 14:42] installed pkgconfig (0.23-2)
[2010-05-28 14:42] installed ar9170-fw (1.0-2)
[2010-05-28 14:42] installed b43-fwcutter (013-1)
[2010-05-28 14:42] installed bridge-utils (1.4-3)
[2010-05-28 14:42] installed run-parts (3.2.2-1)
[2010-05-28 12:42] Clearing symlinks in /etc/ssl/certs...done.
[2010-05-28 12:42] Updating certificates in /etc/ssl/certs... 141 added, 0 removed; done.
[2010-05-28 12:42] Running hooks in /etc/ca-certificates/update.d....done.
[2010-05-28 14:42] installed ca-certificates (20090814-3)
[2010-05-28 14:42] installed wireless-regdb (2009.11.25-1)
[2010-05-28 14:42] installed iw (0.9.18-1)
[2010-05-28 12:42] Uncomment the right regulatory domain in /etc/conf.d/wireless-regdom.
[2010-05-28 12:42] It will automatically be set when necessary.
[2010-05-28 14:42] installed crda (1.1.0-1)
[2010-05-28 14:42] installed dialog (1.1_20100119-2)
[2010-05-28 14:42] installed dmraid (1.0.0.rc16+CVS-2)
[2010-05-28 14:42] installed dnsutils (9.6.1-3)
[2010-05-28 14:42] installed gcc-ada (4.5.0-1)
[2010-05-28 14:42] installed gcc-fortran (4.5.0-1)
[2010-05-28 14:42] installed gcc-objc (4.5.0-1)
[2010-05-28 14:42] installed gpm (1.20.6-5)
[2010-05-28 14:42] installed hdparm (9.28-1)
[2010-05-28 14:42] installed sqlite3 (3.6.23.1-1)
[2010-05-28 14:42] installed heimdal (1.3.2-1)
[2010-05-28 14:42] installed ifenslave (1.1.0-5)
[2010-05-28 14:42] installed inetutils (1.7-3)
[2010-05-28 14:42] installed linux-atm (2.5.1-1)
[2010-05-28 14:42] installed iproute2 (2.6.33-1)
[2010-05-28 14:42] installed iptables (1.4.7-1)
[2010-05-28 14:42] installed kernel26-headers (2.6.33.4-1)
[2010-05-28 14:42] installed udev-compat (151-3)
[2010-05-28 12:42] >>> Updating module dependencies. Please wait ...
[2010-05-28 12:42] >>> MKINITCPIO SETUP
[2010-05-28 12:42] >>> -----------------
[2010-05-28 12:42] >>> If you use LVM2, Encrypted root or software RAID,
[2010-05-28 12:42] >>> Ensure you enable support in /etc/mkinitcpio.conf .
[2010-05-28 12:42] >>> More information about mkinitcpio setup can be found here:
[2010-05-28 12:42] >>> http://wiki.archlinux.org/index.php/Mkinitcpio
[2010-05-28 12:42]
[2010-05-28 12:42] >>> Generating initial ramdisk, using mkinitcpio.  Please wait...
[2010-05-28 12:42] > Building image "default"
[2010-05-28 12:42] > Running command: /sbin/mkinitcpio -k 2.6.27-lts -c /etc/mkinitcpio.conf -g /boot
[2010-05-28 12:42] :: Begin build
```

```
[2010-05-28 12:42] :: Parsing hook [base]
[2010-05-28 12:42] :: Parsing hook [udev]
[2010-05-28 12:42] :: Parsing hook [autodetect]
[2010-05-28 12:42] :: Parsing hook [pata]
[2010-05-28 12:42] :: Parsing hook [scsi]
[2010-05-28 12:42] :: Parsing hook [sata]
[2010-05-28 12:42] :: Parsing hook [filesystems]
[2010-05-28 12:42] :: Generating module dependencies
[2010-05-28 12:42] :: Generating image '/boot/kernel26-lts.img'...SUCCESS
[2010-05-28 12:42] > SUCCESS
[2010-05-28 12:42] > Building image "fallback"
[2010-05-28 12:42] > Running command: /sbin/mkinitcpio -k 2.6.27-lts -c /etc/mkinitcpio.conf -g /boot
[2010-05-28 12:42] :: Begin build
[2010-05-28 12:42] :: Parsing hook [base]
[2010-05-28 12:42] :: Parsing hook [udev]
[2010-05-28 12:42] :: Parsing hook [pata]
[2010-05-28 12:42] :: Parsing hook [scsi]
[2010-05-28 12:42] :: Parsing hook [sata]
[2010-05-28 12:42] :: Parsing hook [filesystems]
[2010-05-28 12:42] :: Generating module dependencies
[2010-05-28 12:42] :: Generating image '/boot/kernel26-lts-fallback.img'...SUCCESS
[2010-05-28 12:42] > SUCCESS
[2010-05-28 14:42] installed kernel26-lts (2.6.27.46-1)
[2010-05-28 14:42] installed kernel26-lts-headers (2.6.27.46-1)
[2010-05-28 14:42] installed libevent (1.4.13-1)
[2010-05-28 14:42] installed libgssglue (0.1-2)
[2010-05-28 14:42] installed libsasl (2.1.23-4)
[2010-05-28 14:42] installed libldap (2.4.21-2)
[2010-05-28 14:42] installed librpcsecgss (0.19-3)
[2010-05-28 14:42] installed libtirpc (0.2.1-1)
[2010-05-28 14:42] installed links (2.2-4)
[2010-05-28 14:42] installed mkinitcpio-nfs-utils (0.2-1)
[2010-05-28 12:42] mlocate command is technically locate, but slocate is symlinked and still works.
[2010-05-28 12:42] You should run updatedb as root.
[2010-05-28 14:42] installed mlocate (0.22.4-1)
[2010-05-28 14:42] installed wireless_tools (29-3)
[2010-05-28 14:42] installed netcfg (2.5.4-1)
[2010-05-28 14:42] installed rpcbind (0.2.0-1)
[2010-05-28 14:42] installed nfsidmap (0.23-3)
[2010-05-28 12:42]   > PLEASE NOTE:
[2010-05-28 12:42]   > Extended configuration options for NFS (clients & server) are available in
[2010-05-28 12:42]   > /etc/conf.d/nfs-common.conf and in /etc/conf.d/nfs-server.conf
[2010-05-28 12:42]   >
[2010-05-28 12:42]   > Please refer to http://wiki.archlinux.org/index.php/Nfs
[2010-05-28 12:42]   > for further information on NFS; for NFSv4, refer to
[2010-05-28 12:42]   > http://wiki.archlinux.org/index.php/NFSv4
[2010-05-28 14:42] installed nfs-utils (1.2.2-2)
[2010-05-28 14:42] installed openssh (5.4p1-4)
[2010-05-28 14:42] installed openvpn (2.1.1-2)
[2010-05-28 14:42] installed pptpclient (1.7.2-2)
[2010-05-28 14:42] installed procinfo-ng (2.0.304-1)
[2010-05-28 14:42] installed rfkill (0.4-1)
[2010-05-28 14:42] installed sdparm (1.05-1)
[2010-05-28 14:42] installed sudo (1.7.2p6-1)
[2010-05-28 14:42] installed vpnc (0.5.3-2)
[2010-05-28 14:42] installed wpa_actiond (1.1-1)
[2010-05-28 13:44] synchronizing package lists
[2010-05-28 13:44] starting full system upgrade
```

```
[2010-05-28 13:47] upgraded bash (4.1.005-1 -> 4.1.007-1)
[2010-05-28 13:47] upgraded dash (0.5.5.1-2 -> 0.5.6-1)
[2010-05-28 13:47] upgraded dialog (1.1_20100119-2 -> 1.1_20100428-1)
[2010-05-28 13:47] upgraded e2fsprogs (1.41.11-1 -> 1.41.12-1)
[2010-05-28 13:47] upgraded libmpc (0.8.1-2 -> 0.8.2-1)
[2010-05-28 13:47] upgraded gcc (4.5.0-1 -> 4.5.0-2)
[2010-05-28 13:47] upgraded gcc-ada (4.5.0-1 -> 4.5.0-2)
[2010-05-28 13:47] upgraded gcc-fortran (4.5.0-1 -> 4.5.0-2)
[2010-05-28 13:47] upgraded gcc-libs (4.5.0-1 -> 4.5.0-2)
[2010-05-28 13:47] upgraded gcc-objc (4.5.0-1 -> 4.5.0-2)
[2010-05-28 13:47] upgraded gettext (0.17-4 -> 0.18-1)
[2010-05-28 13:47] upgraded inetutils (1.7-3 -> 1.8-1)
[2010-05-28 13:47] upgraded openssh (5.4p1-4 -> 5.5p1-1)
[2010-05-28 13:47] upgraded syslog-ng (3.1.0-1 -> 3.1.1-1)
[2010-05-28 13:47] upgraded tar (1.23-1 -> 1.23-2)
[2010-05-28 16:04] installed xcb-proto (1.6-1)
[2010-05-28 16:04] installed xproto (7.0.17-1)
[2010-05-28 16:04] installed libxdmcp (1.0.3-1)
[2010-05-28 16:04] installed libxau (1.0.5-1)
[2010-05-28 16:04] installed libxcb (1.6-1)
[2010-05-28 16:04] installed kbproto (1.0.4-1)
[2010-05-28 16:04] installed libx11 (1.3.3-1)
[2010-05-28 16:04] installed xextproto (7.1.1-1)
[2010-05-28 16:04] installed fixesproto (4.1.1-1)
[2010-05-28 16:04] installed libxfixes (4.0.4-1)
[2010-05-28 16:04] installed renderproto (0.11-1)
[2010-05-28 16:04] installed libxrender (0.9.5-1)
[2010-05-28 16:04] installed libxcursor (1.1.10-1)
[2010-05-28 16:04] installed libxkbfile (1.0.6-1)
[2010-05-28 16:04] installed libpng (1.4.2-1)
[2010-05-28 16:04] installed freetype2 (2.3.12-1)
[2010-05-28 16:04] updating font cache... done.
[2010-05-28 16:04] installed fontconfig (2.8.0-1)
[2010-05-28 16:04] installed libxft (2.1.14-1)
[2010-05-28 16:04] installed libfontenc (1.0.5-1)
[2010-05-28 16:04] installed libxext (1.1.1-1)
[2010-05-28 16:04] installed libice (1.0.6-1)
[2010-05-28 16:04] installed libsm (1.1.1-1)
[2010-05-28 16:04] installed libxt (1.0.8-1)
[2010-05-28 16:04] installed libxmu (1.0.5-1)
[2010-05-28 16:04] installed libxpm (3.5.8-1)
[2010-05-28 16:04] installed libxaw (1.0.7-1)
[2010-05-28 16:04] installed xorg-apps (7.5-3)
[2010-05-28 16:04] installed xorg-xkb-utils (7.5-2)
[2010-05-28 16:04] installed damageproto (1.2.0-1)
[2010-05-28 16:04] installed libxdamage (1.1.2-1)
[2010-05-28 16:04] installed libdrm (2.4.19-2)
[2010-05-28 16:04] installed xf86vidmodeproto (2.3-1)
[2010-05-28 16:04] installed libxxf86vm (1.1.0-1)
[2010-05-28 16:04] installed libgl (7.7.1-1)
[2010-05-28 16:04] installed videoproto (2.3.0-1)
[2010-05-28 16:04] installed libxv (1.0.5-1)
[2010-05-28 16:04] installed libxvmc (1.0.5-1)
[2010-05-28 16:04] installed audiofile (0.2.7-1)
[2010-05-28 16:04] installed alsa-lib (1.0.23-1)
[2010-05-28 16:04] installed esound (0.2.41-1)
[2010-05-28 16:04] installed libogg (1.2.0-1)
[2010-05-28 16:04] installed flac (1.2.1-2)
```

```
[2010-05-28 16:04] installed libvorbis (1.3.1-1)
[2010-05-28 16:04] installed sdl (1.2.14-4)
[2010-05-28 16:04] installed libjpeg (8.0.1-1)
[2010-05-28 16:04] installed libmng (1.0.10-3)
[2010-05-28 16:04] installed libtheora (1.1.1-1)
[2010-05-28 16:04] installed wavpack (4.60.1-1)
[2010-05-28 16:04] installed faad2 (2.7-1)
[2010-05-28 16:04] installed lame (3.98.4-1)
[2010-05-28 16:04] installed libmp4v2 (1.9.1-1)
[2010-05-28 16:04] installed faac (1.28-2)
[2010-05-28 16:04] installed xvidcore (1.2.2-1)
[2010-05-28 16:04] installed x264 (20100524-1)
[2010-05-28 16:04] installed opencore-amr (0.1.2-1)
[2010-05-28 16:04] installed libvdpau (0.4-1)
[2010-05-28 16:04] installed orc (0.4.4-1)
[2010-05-28 16:04] installed schroedinger (1.0.9-1)
[2010-05-28 16:04] installed ffmpeg (23328-1)
[2010-05-28 16:04] installed xine-lib (1.1.18.1-1)
[2010-05-28 16:04] installed atk (1.30.0-1)
[2010-05-28 16:04] installed pixman (0.18.2-1)
[2010-05-28 16:04] installed xcb-util (0.3.6-1)
[2010-05-28 16:04] installed cairo (1.8.10-1)
[2010-05-28 16:04] installed libdatrie (0.2.3-1)
[2010-05-28 16:04] installed libthai (0.1.14-1)
[2010-05-28 16:04] installed pango (1.28.0-1)
[2010-05-28 16:04] installed xineramaproto (1.2-1)
[2010-05-28 16:04] installed libxinerama (1.1-1)
[2010-05-28 16:04] installed randrproto (1.3.1-1)
[2010-05-28 16:04] installed libxrandr (1.3.0-1)
[2010-05-28 16:04] installed inputproto (2.0-1)
[2010-05-28 16:04] installed libxi (1.3-2)
[2010-05-28 16:04] installed compositeproto (0.4.1-1)
[2010-05-28 16:04] installed libxcomposite (0.4.1-1)
[2010-05-28 16:04] installed libtasn1 (2.6-1)
[2010-05-28 16:04] installed gnutls (2.8.6-1)
[2010-05-28 16:04] installed libxml2 (2.7.7-1)
[2010-05-28 16:04] installed shared-mime-info (0.71-1)
[2010-05-28 16:04] installed libtiff (3.9.2-2)
[2010-05-28 16:04] installed dbus (1.2.24-1)
[2010-05-28 16:04] installed libdaemon (0.14-1)
[2010-05-28 16:04] adding avahi system group... adding avahi system user... > The following daemons r
[2010-05-28 16:04]  -> avahi-daemon   - the mdns responder, you probably want this.
[2010-05-28 16:04]                      dbus needs to be running when you start it.
[2010-05-28 16:04]  -> avahi-dnsconfd - daemon used for peer-to-peer automatic dns
[2010-05-28 16:04]                      configuration on dhcp-less networks.
[2010-05-28 16:04]
[2010-05-28 16:04] > To use some of the client applications you will have to install python.
[2010-05-28 16:04]  -> In addition, pygtk is required for the graphical ones and
[2010-05-28 16:04]     twisted-web for avahi-bookmarks.
[2010-05-28 16:04]
[2010-05-28 16:04] installed avahi (0.6.25-3)
[2010-05-28 16:04] installed libcups (1.4.3-2)
[2010-05-28 16:04] installed gtk2 (2.20.1-2)
[2010-05-28 16:04] installed nspr (4.8.4-1)
[2010-05-28 16:04] installed spidermonkey (1.7.0-3)
[2010-05-28 16:04] installed dbus-glib (0.86-1)
[2010-05-28 16:04] installed hal-info (0.20091130-1)
[2010-05-28 16:04] installed eject (2.1.5-4)
```

```
[2010-05-28 16:04] installed dmidecode (2.10-1)
[2010-05-28 16:04] installed libx86 (1.1-2)
[2010-05-28 16:04] installed vbetool (1.1-1)
[2010-05-28 16:04] installed pm-quirks (0.20100316-1)
[2010-05-28 16:04] installed pm-utils (1.3.0-2)
[2010-05-28 16:04] installed eggdbus (0.6-1)
[2010-05-28 16:04] installed polkit (0.96-2)
[2010-05-28 16:04] installed consolekit (0.4.1-2)
[2010-05-28 16:04] installed hal (0.5.14-2)
[2010-05-28 16:04] installed desktop-file-utils (0.16-1)
[2010-05-28 16:04] installed hicolor-icon-theme (0.12-1)
[2010-05-28 16:04] installed gxine (0.5.905-1)
[2010-05-28 16:04] installed alsaplayer (0.99.80-3)
[2010-05-28 16:04] installed alsa-utils (1.0.23-2)
[2010-05-28 16:04] Install jack-audio-connection-kit, libsamplerate, ffmpeg
[2010-05-28 16:04] or pulseaudio to get their respective plugins working
[2010-05-28 16:04] installed alsa-plugins (1.0.23-1)
[2010-05-28 16:04] installed acpi (1.4-2)
[2010-05-28 16:04] installed acpid (1.0.10-3)
[2010-05-28 16:04] installed libstdc++5 (3.3.6-3)
[2010-05-28 16:04] installed acpitool (0.5.1-1)
[2010-05-28 16:04] installed rrdtool (1.4.3-1)
[2010-05-28 16:04] warning: /etc/sensors3.conf saved as /etc/sensors3.conf.pacorig
[2010-05-28 16:04] >>> to control the lm_sensors daemon type
[2010-05-28 16:04] >>> "/etc/rc.d/sensors start|stop|restart"
[2010-05-28 16:04] >>> --------------------------------------
[2010-05-28 16:04] >>> before you can use the fancontrol daemon
[2010-05-28 16:04] >>> first create a fancontrol config file, use "pwmconfig"
[2010-05-28 16:04] >>> then type "/etc/rc.d/fancontrol start|stop|restart"
[2010-05-28 16:04] >>> --------------------------------------
[2010-05-28 16:04] >>> to decode memory SPD timings modprobe eeprom module
[2010-05-28 16:04] >>> and get this perl script from
[2010-05-28 16:04] >>> "http://www.lm-sensors.org/browser/lm-sensors/trunk/prog/eeprom/decode-dimms.p
[2010-05-28 16:04] installed lm_sensors (3.1.2-3)
[2010-05-28 16:04] installed smartmontools (5.39.1-1)
[2010-05-28 16:04] installed neon (0.29.3-2)
[2010-05-28 16:04] installed apr (1.4.2-1)
[2010-05-28 16:04] installed unixodbc (2.3.0-1)
[2010-05-28 16:04] installed apr-util (1.3.9-4)
[2010-05-28 16:04] installed subversion (1.6.9-5)
[2010-05-28 16:04] installed python (2.6.5-3)
[2010-05-28 16:04] installed ruby (1.9.1_p378-2)
[2010-05-28 16:04] installed ntp (4.2.6-3)
[2010-05-28 16:04] installed curl (7.20.1-1)
[2010-05-28 16:04] installed hunspell (1.2.11-1)
[2010-05-28 16:04] installed libgsf (1.14.18-1)
[2010-05-28 16:04] installed libwpd (0.8.14-1)
[2010-05-28 16:04] installed icu (4.4.1-1)
[2010-05-28 16:04] installed hsqldb-java (1.8.1.2-1)
[2010-05-28 16:04] installed libxslt (1.1.26-1)
[2010-05-28 16:04] installed recordproto (1.14-1)
[2010-05-28 16:04] installed libxtst (1.1.0-1)
[2010-05-28 16:04] The jre package is licensed software.
[2010-05-28 16:04] You MUST read and agree to the license stored in
[2010-05-28 16:04] /opt/java/jre/LICENSE before using it.
[2010-05-28 16:04] installed jre (6u20-1)
[2010-05-28 16:04] installed beanshell (2.0b4-1)
[2010-05-28 16:04] installed saxon (9.2.0.6-1)
```

```
[2010-05-28 16:04] installed hdf5 (1.8.4_patch1-1)
[2010-05-28 16:04] installed fftw (3.2.2-1)
[2010-05-28 16:04] installed vigra (1.7.0-1)
[2010-05-28 16:04] installed libgraphite (2.3.1-1)
[2010-05-28 16:04] installed hyphen (2.5-1)
[2010-05-28 16:04] installed lpsolve (5.5.0.15-1)
[2010-05-28 16:04] installed libmspack (0.0.20060920alpha-2)
[2010-05-28 16:04] installed lucene (2.9.2-1)
[2010-05-28 16:04]  * check /etc/profile.d/openoffice.sh, then relogin or "source" the file
[2010-05-28 16:04]  * see http://wiki.archlinux.org/index.php/Openoffice
[2010-05-28 16:04]    how to use extensions, e.g. for spell checking
[2010-05-28 16:04]    see /usr/lib/openoffice/share/extension/install what
[2010-05-28 16:04]    is shipped with this package
[2010-05-28 16:04]  * make sure you have installed a ttf font (ttf-dejavu recommended)
[2010-05-28 16:04] installed openoffice-base (3.2.0-3)
[2010-05-28 16:04] installed openoffice-de (3.2.0-1)
[2010-05-28 16:04] installed vuze (4.4.0.4-1)
[2010-05-28 16:04] relogin or source /etc/profile.d/mozilla-common.sh
[2010-05-28 16:04] installed mozilla-common (1.4-1)
[2010-05-28 16:04] installed nss (3.12.6-3)
[2010-05-28 16:04] installed flashplugin (10.0.45.2-1)
[2010-05-28 16:04] installed libidl2 (0.8.14-1)
[2010-05-28 16:04] installed orbit2 (2.14.18-1)
[2010-05-28 16:04] installed gconf (2.28.1-1)
[2010-05-28 16:04] installed gtksourceview2 (2.10.1-1)
[2010-05-28 16:04] installed libglade (2.6.4-1)
[2010-05-28 16:04] installed pycairo (1.8.8-1)
[2010-05-28 16:04] installed libffi (3.0.9-1)
[2010-05-28 16:04] installed pygobject (2.21.1-1)
[2010-05-28 16:04] installed pygtk (2.17.0-1)
[2010-05-28 16:04] installed pygtksourceview2 (2.10.1-1)
[2010-05-28 16:04] > aspell comes with no default dictionary
[2010-05-28 16:04] installed aspell (0.60.6-4)
[2010-05-28 16:04] installed enchant (1.6.0-1)
[2010-05-28 16:04] installed iso-codes (3.14-1)
[2010-05-28 16:04] installed gedit (2.30.2-1)
[2010-05-28 16:04] installed vte (0.24.1-1)
[2010-05-28 16:04] installed gucharmap (2.30.1-1)
[2010-05-28 16:04] installed pyorbit (2.24.0-2)
[2010-05-28 16:04] installed libart-lgpl (2.3.21-1)
[2010-05-28 16:04] installed libgnomecanvas (2.30.1-1)
[2010-05-28 16:04] installed fam (2.7.0-14)
[2010-05-28 16:04] installed tdb (1.2.1-1)
[2010-05-28 16:04] installed talloc (2.0.1-1)
[2010-05-28 16:04] installed smbclient (3.5.2-1)
[2010-05-28 16:04] installed gnome-mime-data (2.18.0-4)
[2010-05-28 16:04] installed gnome-vfs (2.24.3-2)
[2010-05-28 16:04] installed libbonobo (2.24.3-1)
[2010-05-28 16:04] installed gnome-keyring (2.30.1-2)
[2010-05-28 16:04] installed libgnome-keyring (2.30.1-1)
[2010-05-28 16:04] installed libsoup (2.30.1-1)
[2010-05-28 16:04] installed libproxy (0.3.1-1)
[2010-05-28 16:04] installed libsoup-gnome (2.30.1-1)
[2010-05-28 16:04] installed libunique (1.1.6-2)
[2010-05-28 16:04] installed sg3_utils (1.28-1)
[2010-05-28 16:04] installed parted (2.2-1)
[2010-05-28 16:04] installed libatasmart (0.17-1)
[2010-05-28 16:04] installed lsof (4.83-1)
```

```
[2010-05-28 16:04] installed udisks (1.0.1-1)
[2010-05-28 16:04] installed libnotify (0.4.5-1)
[2010-05-28 16:04] installed gnome-disk-utility (2.30.1-1)
[2010-05-28 16:04] installed libcddb (1.3.2-2)
[2010-05-28 16:04] installed libcdio (0.82-1)
[2010-05-28 16:04] > You must load the fuse kernel module to use FUSE.
[2010-05-28 16:04]  -> Run 'modprobe fuse' to load the module now.
[2010-05-28 16:04]  -> Add fuse to $MODULES in /etc/rc.conf to load on every boot.
[2010-05-28 16:04] > You will need a /dev/fuse device node to use FUSE.
[2010-05-28 16:04]  -> If you use udev, nothing needs to be done
[2010-05-28 16:04]  -> For a static /dev, run: mknod /dev/fuse -m 0666 c 10 229
[2010-05-28 16:04] installed fuse (2.8.4-1)
[2010-05-28 16:04] installed gvfs (1.6.2-1)
[2010-05-28 16:05] installed libgnome (2.30.0-1)
[2010-05-28 16:05] installed libbonoboui (2.24.3-1)
[2010-05-28 16:05] installed libgnomeui (2.24.3-1)
[2010-05-28 16:05] installed gnome-python (2.28.1-1)
[2010-05-28 16:05] installed gedit-plugins (2.30.0-1)
[2010-05-28 16:05] installed dbus-python (0.83.1-1)
[2010-05-28 16:05] installed gedit-plugins-extra (2.24.1-5)
[2010-05-28 16:05] installed giflib (4.1.6-3)
[2010-05-28 16:05] installed libid3tag (0.15.1b-4)
[2010-05-28 16:05] installed imlib2 (1.4.4-1)
[2010-05-28 16:05] installed fluxbox (1.1.1-1)
[2010-05-28 16:05] installed unzip (6.0-5)
[2010-05-28 16:05] installed unrar (3.9.10-1)
[2010-05-28 16:05] installed htop (0.8.3-1)
[2010-05-28 16:05] installed wireshark (1.2.8-1)
[2010-05-28 16:05] installed zsh (4.3.10-3)
[2010-05-28 16:05] installed sdl_ttf (2.0.9-2)
[2010-05-28 16:05] installed sdl_net (1.2.7-3)
[2010-05-28 16:05] installed libmikmod (3.1.12-3)
[2010-05-28 16:05] installed smpeg (0.4.4-5)
[2010-05-28 16:05] installed sdl_mixer (1.2.11-2)
[2010-05-28 16:05] installed sdl_image (1.2.10-2)
[2010-05-28 16:05] installed fribidi (0.19.2-1)
[2010-05-28 16:05] installed boost (1.41.0-1)
[2010-05-28 16:05] installed lua (5.1.4-4)
[2010-05-28 16:05] Note:
[2010-05-28 16:05] > If you experience sound problems try setting your SDL_AUDIODRIVER environment va
[2010-05-28 16:05] > eg. export SDL_AUDIODRIVER="dma" ; wesnoth
[2010-05-28 16:05] > If "dma" doesn't work,other options are: dsp,alsa,artsc,esd,nas try to find the
[2010-05-28 16:05] installed wesnoth (1.8.1-1)
[2010-05-28 16:05] installed gd (2.0.36RC1-3)
[2010-05-28 16:05] installed libcroco (0.6.2-1)
[2010-05-28 16:05] installed librsvg (2.26.3-1)
[2010-05-28 16:05] installed dri2proto (2.1-2)
[2010-05-28 16:05] installed mesa (7.7.1-1)
[2010-05-28 16:05] installed freeglut (2.6.0-1)
[2010-05-28 16:05] installed jasper (1.900.1-5)
[2010-05-28 16:05] installed ghostscript (8.71-3)
[2010-05-28 16:05] installed graphviz (2.26.3-1)
[2010-05-28 16:06] The jdk package is licensed software.
[2010-05-28 16:06] You MUST read and agree to the license stored in
[2010-05-28 16:06] /opt/java/LICENSE before using it.
[2010-05-28 16:06] installed jdk (6u20-1)
[2010-05-28 16:06] installed startup-notification (0.10-1)
[2010-05-28 16:06] warning: /etc/mime.types saved as /etc/mime.types.pacorig
```

```
[2010-05-28 16:06] installed mime-types (1.0-3)
[2010-05-28 16:06] installed xulrunner (1.9.2.3-1)
[2010-05-28 16:06] installed firefox (3.6.3-1)
[2010-05-28 16:06] installed thunderbird (3.0.4-1)
[2010-05-28 16:06] installed eclipse (3.5.2-1)
[2010-05-28 16:06] installed eclipse-cdt (6.0.2-1)
[2010-05-28 16:06] installed lcms (1.18-3)
[2010-05-28 16:06] installed fontsproto (2.1.0-1)
[2010-05-28 16:06] installed libxfont (1.4.1-1)
[2010-05-28 16:06] installed xorg-font-utils (7.5-2)
[2010-05-28 16:06] Updating font cache... done.
[2010-05-28 16:06] installed gsfonts (1.0.7pre44-2)
[2010-05-28 16:06] installed libwmf (0.2.8.4-7)
[2010-05-28 16:06] installed libexif (0.6.19-1)
[2010-05-28 16:06] installed babl (0.1.2-1)
[2010-05-28 16:06] installed gegl (0.1.2-1)
[2010-05-28 16:06] installed gimp (2.6.8-4)
[2010-05-28 16:06] installed kdeaccessibility-colorschemes (4.4.3-1)
[2010-05-28 16:06] installed kdeaccessibility-iconthemes (4.4.3-1)
[2010-05-28 16:06] installed ilmbase (1.0.1-1)
[2010-05-28 16:06] installed openexr (1.6.1-1)
[2010-05-28 16:06] installed xdg-utils (1.0.2.20100303-1)
[2010-05-28 16:06] installed qt (4.6.2-4)
[2010-05-28 16:06] installed clucene (0.9.21b-1)
[2010-05-28 16:06] installed exiv2 (0.19-1)
[2010-05-28 16:06] installed strigi (0.7.2-2)
[2010-05-28 16:06] installed raptor (1.4.21-1)
[2010-05-28 16:06] installed postgresql-libs (8.4.4-1)
[2010-05-28 16:06] installed libmysqlclient (5.1.46-2)
[2010-05-28 16:06] installed rasqal (0.9.19-1)
[2010-05-28 16:06] installed redland (1.0.10-2)
[2010-05-28 16:06] installed libiodbc (3.52.7-3)
[2010-05-28 16:06] installed virtuoso (6.1.1-1)
[2010-05-28 16:06] installed soprano (2.4.3-1)
[2010-05-28 16:06] installed qca (2.0.2-2)
[2010-05-28 16:06] installed polkit-qt (0.95.1-1)
[2010-05-28 16:06] installed scrnsaverproto (1.2.0-1)
[2010-05-28 16:06] installed libxss (1.2.0-1)
[2010-05-28 16:06] installed gstreamer0.10 (0.10.29-1)
[2010-05-28 16:06] installed liboil (0.3.17-1)
[2010-05-28 16:06] installed gstreamer0.10-base (0.10.29-1)
[2010-05-28 16:06] installed cdparanoia (10.2-2)
[2010-05-28 16:06] installed libvisual (0.4.0-3)
[2010-05-28 16:06] installed gstreamer0.10-base-plugins (0.10.29-1)
[2010-05-28 16:06] installed phonon-gstreamer (4.4.1-1)
[2010-05-28 16:06] installed phonon (4.4.1-1)
[2010-05-28 16:06] installed shared-desktop-ontologies (0.5-1)
[2010-05-28 16:06] installed attica (0.1.4-1)
[2010-05-28 16:07] installed kdelibs (4.4.3-2)
[2010-05-28 16:07] installed oxygen-icons (4.4.3-1)
[2010-05-28 16:07] installed xorg-xauth (1.0.4-1)
[2010-05-28 16:07] installed rarian (0.8.1-1)
[2010-05-28 16:07] installed libssh (0.4.1-3)
[2010-05-28 16:07] installed kdebase-runtime (4.4.3-1)
[2010-05-28 16:07] installed kdeaccessibility-kmag (4.4.3-1)
[2010-05-28 16:07] installed kdeaccessibility-kmousetool (4.4.3-1)
[2010-05-28 16:07] installed kdeaccessibility-kmouth (4.4.3-1)
[2010-05-28 16:07] installed kdeadmin-kcron (4.4.3-1)
```

```
[2010-05-28 16:07] installed kdeadmin-ksystemlog (4.4.3-1)
[2010-05-28 16:07] installed mysql-clients (5.1.46-2)
[2010-05-28 16:07] warning: /etc/mysql/my.cnf saved as /etc/mysql/my.cnf.pacorig
[2010-05-28 16:07] WARNING: The host 'Lab1' could not be looked up with resolveip.
[2010-05-28 16:07] This probably means that your libc libraries are not 100 % compatible
[2010-05-28 16:07] with this binary MySQL version. The MySQL daemon, mysqld, should work
[2010-05-28 16:07] normally with the exception that host name resolving will not work.
[2010-05-28 16:07] This means that you should use IP addresses instead of hostnames
[2010-05-28 16:07] when specifying MySQL privileges !
[2010-05-28 16:07] Installing MySQL system tables...
[2010-05-28 16:07] OK
[2010-05-28 16:07] Filling help tables...
[2010-05-28 16:07] OK
[2010-05-28 16:07]
[2010-05-28 16:07] To start mysqld at boot time you have to copy
[2010-05-28 16:07] support-files/mysql.server to the right place for your system
[2010-05-28 16:07]
[2010-05-28 16:07] PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
[2010-05-28 16:07] To do so, start the server, then issue the following commands:
[2010-05-28 16:07]
[2010-05-28 16:07] /usr/bin/mysqladmin -u root password 'new-password'
[2010-05-28 16:07] /usr/bin/mysqladmin -u root -h Lab1 password 'new-password'
[2010-05-28 16:07]
[2010-05-28 16:07] Alternatively you can run:
[2010-05-28 16:07] /usr/bin/mysql_secure_installation
[2010-05-28 16:07]
[2010-05-28 16:07] which will also give you the option of removing the test
[2010-05-28 16:07] databases and anonymous user created by default.  This is
[2010-05-28 16:07] strongly recommended for production servers.
[2010-05-28 16:07]
[2010-05-28 16:07] See the manual for more instructions.
[2010-05-28 16:07]
[2010-05-28 16:07] You can start the MySQL daemon with:
[2010-05-28 16:07] cd /usr ; /usr/bin/mysqld_safe &
[2010-05-28 16:07]
[2010-05-28 16:07] You can test the MySQL daemon with mysql-test-run.pl
[2010-05-28 16:07] cd /usr/mysql-test ; perl mysql-test-run.pl
[2010-05-28 16:07]
[2010-05-28 16:07] Please report any problems with the /usr/bin/mysqlbug script!
[2010-05-28 16:07]
[2010-05-28 16:07] installed mysql (5.1.46-2)
[2010-05-28 16:07] installed akonadi (1.3.1-3)
[2010-05-28 16:07] installed libical (0.44-1)
[2010-05-28 16:07] installed pth (2.0.7-3)
[2010-05-28 16:07] installed gnupg (1.4.10-2)
[2010-05-28 16:07] installed libksba (1.0.7-1)
[2010-05-28 16:07] installed libassuan (2.0.0-1)
[2010-05-28 16:07] installed pinentry (0.8.0-1)
[2010-05-28 16:07] installed dirmngr (1.1.0rc1-1)
[2010-05-28 16:07] installed gnupg2 (2.0.15-1)
[2010-05-28 16:07] installed gpgme (1.3.0-1)
[2010-05-28 16:07] installed kdepimlibs (4.4.3-1)
[2010-05-28 16:07] installed kdepim-runtime (4.4.3-1)
[2010-05-28 16:07] installed kdeadmin-kuser (4.4.3-1)
[2010-05-28 16:07] installed sip (4.10.2-1)
[2010-05-28 16:07] installed qscintilla (2.4.3-1)
[2010-05-28 16:07] installed pyqt (4.7.3-1)
[2010-05-28 16:07] installed kdebindings-python (4.4.3-1)
```

```
[2010-05-28 16:07] installed pycups (1.9.49-1)
[2010-05-28 16:07] installed pysmbc (1.0.6-3)
[2010-05-28 16:07] installed system-config-printer-common (1.2.1-1)
[2010-05-28 16:07] installed kdeadmin-system-config-printer-kde (4.4.3-1)
[2010-05-28 16:07] installed kdeartwork-colorschemes (4.4.3-1)
[2010-05-28 16:07] installed kdeartwork-desktopthemes (4.4.3-1)
[2010-05-28 16:07] installed kdeartwork-emoticons (4.4.3-1)
[2010-05-28 16:07] installed kdeartwork-iconthemes (4.4.3-1)
[2010-05-28 16:07] installed polkit-kde (0.95.1-2)
[2010-05-28 16:07] installed qimageblitz (0.0.5-1)
[2010-05-28 16:07] installed xf86miscproto (0.9.3-1)
[2010-05-28 16:07] installed libxxf86misc (1.0.2-1)
[2010-05-28 16:07] installed xkeyboard-config (1.8-1)
[2010-05-28 16:07] installed libxklavier (5.0-1)
[2010-05-28 16:07] installed xf86dgaproto (2.1-1)
[2010-05-28 16:07] installed libxxf86dga (1.1.1-1)
[2010-05-28 16:07] installed dmxproto (2.3-1)
[2010-05-28 16:07] installed libdmx (1.1.0-1)
[2010-05-28 16:07] installed xorg-utils (7.6-1)
[2010-05-28 16:07] installed kdebase-workspace (4.4.3-2)
[2010-05-28 16:07] installed kdeartwork-kscreensaver (4.4.3-1)
[2010-05-28 16:07] installed kdeartwork-sounds (4.4.3-1)
[2010-05-28 16:07] installed kdeartwork-styles (4.4.3-1)
[2010-05-28 16:07] installed kdeartwork-wallpapers (4.4.3-1)
[2010-05-28 16:07] installed kdeartwork-weatherwallpapers (4.4.3-1)
[2010-05-28 16:07] installed kdebase-lib (4.4.3-1)
[2010-05-28 16:07] installed kdebase-dolphin (4.4.3-1)
[2010-05-28 16:07] installed kdebase-kappfinder (4.4.3-1)
[2010-05-28 16:07] installed kdebase-kdepasswd (4.4.3-1)
[2010-05-28 16:07] installed kdebase-kdialog (4.4.3-1)
[2010-05-28 16:07] installed kdebase-kfind (4.4.3-1)
[2010-05-28 16:07] installed libraw1394 (2.0.5-1)
[2010-05-28 16:07] installed kdebase-kinfocenter (4.4.3-1)
[2010-05-28 16:07] installed kdebase-konqueror (4.4.3-1)
[2010-05-28 16:07] installed kdebase-konsole (4.4.3-1)
[2010-05-28 16:07] installed kdebase-kwrite (4.4.3-1)
[2010-05-28 16:07] installed kdebase-plasma (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-libkdeedu (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-blinken (4.4.3-1)
[2010-05-28 16:07] installed libspectre (0.2.4-1)
[2010-05-28 16:07] installed kdeedu-cantor (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-kalgebra (4.4.3-1)
[2010-05-28 16:07] installed openbabel (2.2.3-1)
[2010-05-28 16:07] installed kdeedu-kalzium (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-data (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-kanagram (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-kbruch (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-kgeography (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-khangman (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-kig (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-kiten (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-klettres (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-kmplot (4.4.3-1)
[2010-05-28 16:07] installed libnova (0.13.0-1)
[2010-05-28 16:07] installed cfitsio (3240-1)
[2010-05-28 16:07] installed libindi (0.6.1-1)
[2010-05-28 16:07] installed kdeedu-kstars (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-ktouch (4.4.3-1)
```

```
[2010-05-28 16:07] installed kdeedu-kturtle (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-kwordquiz (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-marble (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-parley (4.4.3-1)
[2010-05-28 16:07] installed kdeedu-rocs (4.4.3-1)
[2010-05-28 16:07] installed gsl (1.14-1)
[2010-05-28 16:07] installed cln (1.2.2-3)
[2010-05-28 16:07] installed libqalculate (0.9.7-1)
[2010-05-28 16:07] installed kdeedu-step (4.4.3-1)
[2010-05-28 16:07] installed kdegames-libkdegames (4.4.3-1)
[2010-05-28 16:07] installed kdegames-bomber (4.4.3-1)
[2010-05-28 16:07] installed kdegames-bovo (4.4.3-1)
[2010-05-28 16:08] installed kdegames-granatier (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kapman (4.4.3-1)
[2010-05-28 16:08] installed kdegames-katomic (4.4.3-1)
[2010-05-28 16:08] installed libggz (0.0.14.1-1)
[2010-05-28 16:08] installed ggz-client-libs (0.0.14.1-1)
[2010-05-28 16:08] installed kdegames-kbattleship (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kblackbox (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kblocks (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kbounce (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kbreakout (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kdiamond (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kfourinline (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kgoldrunner (4.4.3-1)
[2010-05-28 16:08] installed gnugo (3.8-1)
[2010-05-28 16:08] installed kdegames-kigo (4.4.3-1)
[2010-05-28 16:08] installed kdegames-killbots (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kiriki (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kjumpingcube (4.4.3-1)
[2010-05-28 16:08] installed kdegames-klines (4.4.3-1)
[2010-05-28 16:08] installed kdegames-libkmahjongg (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kmahjongg (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kmines (4.4.3-1)
[2010-05-28 16:08] installed kdegames-knetwalk (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kolf (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kollision (4.4.3-1)
[2010-05-28 16:08] installed kdegames-konquest (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kpat (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kreversi (4.4.3-1)
[2010-05-28 16:08] installed kdegames-ksame (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kshisen (4.4.3-1)
[2010-05-28 16:08] installed kdegames-ksirk (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kspaceduel (4.4.3-1)
[2010-05-28 16:08] installed kdegames-ksquares (4.4.3-1)
[2010-05-28 16:08] installed kdegames-ksudoku (4.4.3-1)
[2010-05-28 16:08] installed kdegames-ktron (4.4.3-1)
[2010-05-28 16:08] installed kdegames-ktuberling (4.4.3-1)
[2010-05-28 16:08] installed kdegames-kubrick (4.4.3-1)
[2010-05-28 16:08] installed kdegames-lskat (4.4.3-1)
[2010-05-28 16:08] installed kdegames-palapeli (4.4.3-1)
[2010-05-28 16:08] NOTE
[2010-05-28 16:08] ----
[2010-05-28 16:08] Add your user to group 'camera' to use camera devices.
[2010-05-28 16:08] installed libgphoto2 (2.4.9-1)
[2010-05-28 16:08] installed libieee1284 (0.2.11-2)
[2010-05-28 16:08] installed libv4l (0.6.4-1)
[2010-05-28 16:08] warning: /etc/sane.d/epjitsu.conf saved as /etc/sane.d/epjitsu.conf.pacorig
```

```
[2010-05-28 16:08] warning: /etc/sane.d/gt68xx.conf saved as /etc/sane.d/gt68xx.conf.pacorig
[2010-05-28 16:08] warning: /etc/sane.d/genesys.conf saved as /etc/sane.d/genesys.conf.pacorig
[2010-05-28 16:08] warning: /etc/sane.d/canon_dr.conf saved as /etc/sane.d/canon_dr.conf.pacorig
[2010-05-28 16:08] warning: /etc/sane.d/dll.conf saved as /etc/sane.d/dll.conf.pacorig
[2010-05-28 16:08] warning: /etc/sane.d/cardscan.conf saved as /etc/sane.d/cardscan.conf.pacorig
[2010-05-28 16:08] warning: /etc/sane.d/hp3900.conf saved as /etc/sane.d/hp3900.conf.pacorig
[2010-05-28 16:08] warning: /etc/sane.d/fujitsu.conf saved as /etc/sane.d/fujitsu.conf.pacorig
[2010-05-28 16:08] NOTE
[2010-05-28 16:08] ----
[2010-05-28 16:08] Add your user to group 'scanner' to use scanner devices.
[2010-05-28 16:08] installed sane (1.0.21-2)
[2010-05-28 16:08] installed kdegraphics-libs (4.4.3-2)
[2010-05-28 16:08] installed kdegraphics-gwenview (4.4.3-2)
[2010-05-28 16:08] installed kdegraphics-kamera (4.4.3-2)
[2010-05-28 16:08] installed kdegraphics-kcolorchooser (4.4.3-2)
[2010-05-28 16:08] installed kdegraphics-kgamma (4.4.3-2)
[2010-05-28 16:08] installed kdegraphics-kolourpaint (4.4.3-2)
[2010-05-28 16:08] installed kdegraphics-kruler (4.4.3-2)
[2010-05-28 16:08] installed kdegraphics-ksnapshot (4.4.3-2)
[2010-05-28 16:08] installed openjpeg (1.3-3)
[2010-05-28 16:08] installed poppler (0.12.4-1)
[2010-05-28 16:08] installed poppler-qt (0.12.4-1)
[2010-05-28 16:08] installed chmlib (0.40-1)
[2010-05-28 16:08] installed libdjvu (3.5.22-3)
[2010-05-28 16:08] installed libzip (0.9.3-1)
[2010-05-28 16:08] installed ebook-tools (0.1.1-1)
[2010-05-28 16:08] installed kdegraphics-okular (4.4.3-2)
[2010-05-28 16:08] installed kdemultimedia-dragonplayer (4.4.3-1)
[2010-05-28 16:08] installed musicbrainz (2.1.5-3)
[2010-05-28 16:08] installed libmad (0.15.1b-4)
[2010-05-28 16:08] installed libmpcdec (1.2.6-2)
[2010-05-28 16:08] installed libofa (0.9.3-2)
[2010-05-28 16:08] installed taglib (1.6.3-1)
[2010-05-28 16:08] installed tunepimp (0.5.3-7)
[2010-05-28 16:08] installed kdemultimedia-juk (4.4.3-1)
[2010-05-28 16:08] installed kdemultimedia-kioslave (4.4.3-1)
[2010-05-28 16:08] installed kdemultimedia-kmix (4.4.3-1)
[2010-05-28 16:08] installed kdemultimedia-kscd (4.4.3-1)
[2010-05-28 16:08] installed aalib (1.4rc5-6)
[2010-05-28 16:08] installed libsndfile (1.0.21-1)
[2010-05-28 16:08] installed libsamplerate (0.1.7-1)
[2010-05-28 16:08] installed jack (0.118.0-3)
[2010-05-28 16:08] installed libcaca (0.99.beta17-1)
[2010-05-28 16:08] installed libftdi (0.16-1)
[2010-05-28 16:08] installed lirc-utils (0.8.6-3)
[2010-05-28 16:08] Regenerating font encodings... done.
[2010-05-28 16:08] installed xorg-fonts-encodings (1.0.3-1)
[2010-05-28 16:08] installed ttf-dejavu (2.30-2)
[2010-05-28 16:08] installed recode (3.6-4)
[2010-05-28 16:08] installed enca (1.13-1)
[2010-05-28 16:08] installed libdca (0.0.5-2)
[2010-05-28 16:08] installed a52dec (0.7.4-4)
[2010-05-28 16:08] warning: /etc/mplayer/codecs.conf saved as /etc/mplayer/codecs.conf.pacorig
[2010-05-28 16:08] warning: /etc/mplayer/input.conf saved as /etc/mplayer/input.conf.pacorig
[2010-05-28 16:08] installed mplayer (31147-2)
[2010-05-28 16:08] installed kdemultimedia-mplayerthumbs (4.4.3-1)
[2010-05-28 16:08] installed kdenetwork-filesharing (4.4.3-2)
[2010-05-28 16:08] installed kdenetwork-kdnssd (4.4.3-2)
```

```
[2010-05-28 16:08] installed kdenetwork-kget (4.4.3-2)
[2010-05-28 16:08] installed qca-ossl (2.0.0-3)
[2010-05-28 16:08] installed libotr (3.2.0-1)
[2010-05-28 16:08] installed libmsn (4.1-2)
[2010-05-28 16:08] installed libidn (1.16-1)
[2010-05-28 16:08] installed libgadu (1.9.0-1)
[2010-05-28 16:08] installed kdenetwork-kopete (4.4.3-2)
[2010-05-28 16:08] installed kdenetwork-kppp (4.4.3-2)
[2010-05-28 16:08] installed libvncserver (0.9.7-3)
[2010-05-28 16:08] warning: /etc/libao.conf saved as /etc/libao.conf.pacorig
[2010-05-28 16:08] installed libao (1.0.0-1)
[2010-05-28 16:08] installed rdesktop (1.6.0-5)
[2010-05-28 16:08] installed telepathy-glib (0.10.6-1)
[2010-05-28 16:08] installed libnice (0.0.12-1)
[2010-05-28 16:08] installed gstreamer0.10-python (0.10.18-1)
[2010-05-28 16:08] installed farsight2 (0.0.19-1)
[2010-05-28 16:08] installed telepathy-farsight (0.0.14-1)
[2010-05-28 16:08] installed telepathy-qt4 (0.3.3-1)
[2010-05-28 16:08] installed kdenetwork-krdc (4.4.3-2)
[2010-05-28 16:08] installed kdenetwork-krfb (4.4.3-2)
[2010-05-28 16:08] installed kde-agent (20090801-2)
[2010-05-28 16:08] installed kdepim-libkdepim (4.4.3-2)
[2010-05-28 16:08] installed kdepim-akonadiconsole (4.4.3-2)
[2010-05-28 16:08] installed kdepim-akregator (4.4.3-2)
[2010-05-28 16:08] installed kdepim-blogilo (4.4.3-2)
[2010-05-28 16:08] installed kdepim-console (4.4.3-2)
[2010-05-28 16:08] installed kdepim-kaddressbook (4.4.3-2)
[2010-05-28 16:08] installed kdepim-kalarm (4.4.3-2)
[2010-05-28 16:08] installed kdepim-kjots (4.4.3-2)
[2010-05-28 16:08] installed kdepim-kleopatra (4.4.3-2)
[2010-05-28 16:08] installed kdepim-kmail (4.4.3-2)
[2010-05-28 16:08] installed kdepim-knode (4.4.3-2)
[2010-05-28 16:08] installed kdepim-knotes (4.4.3-2)
[2010-05-28 16:08] installed kdepim-korganizer (4.4.3-2)
[2010-05-28 16:08] installed kdepim-kontact (4.4.3-2)
[2010-05-28 16:08] installed kdepim-kresources (4.4.3-2)
[2010-05-28 16:08] installed kdepim-ktimetracker (4.4.3-2)
[2010-05-28 16:08] installed kdepim-wizards (4.4.3-2)
[2010-05-28 16:08] installed kdeplasma-addons-applets-bball (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-binary-clock (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-blackboard (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-bubblemon (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-calculator (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-charselect (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-libs (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-comic (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-dict (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-eyes (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-fifteenpuzzle (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-filewatcher (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-frame (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-fuzzy-clock (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-incomingmsg (4.4.3-1)
[2010-05-28 16:08] installed qwt (5.2.0-2)
[2010-05-28 16:08] installed kdeplasma-addons-applets-kdeobservatory (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-kimpanel (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-knowledgebase (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-kolourpicker (4.4.3-1)
```

```
[2010-05-28 16:08] installed kdeplasma-addons-applets-konqprofiles (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-konsoleprofiles (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-lancelot (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-leavenote (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-life (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-luna (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-magnifique (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-mediaplayer (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-microblog (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-news (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-notes (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-nowplaying (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-opendesktop (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-opendesktop-activities (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-paste (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-pastebin (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-plasmaboard (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-previewer (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-qalculate (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-rememberthemilk (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-rssnow (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-showdashboard (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-showdesktop (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-spellcheck (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-systemloadviewer (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-timer (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-unitconverter (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-weather (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-weatherstation (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-applets-webslice (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-runners-audioplayercontrol (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-runners-browserhistory (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-runners-contacts (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-runners-converter (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-runners-katesessions (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-runners-konquerorsessions (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-runners-konsolesessions (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-runners-kopete (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-runners-mediawiki (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-runners-spellchecker (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-wallpapers-mandelbrot (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-wallpapers-marble (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-wallpapers-pattern (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-wallpapers-virus (4.4.3-1)
[2010-05-28 16:08] installed kdeplasma-addons-wallpapers-weather (4.4.3-1)
[2010-05-28 16:08] installed kdesdk-cervisia (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-kapptemplate (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-kate (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-kbugbuster (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-kcachegrind (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-kdeaccounts-plugin (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-kdepalettes (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-kioslave (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-kmtrace (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-kompare (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-kpartloader (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-kprofilemethod (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-kstartperf (4.4.3-1)
```

```
[2010-05-28 16:09] installed kdesdk-kuiviewer (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-lokalize (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-poxml (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-scripts (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-strigi-analyzer (4.4.3-1)
[2010-05-28 16:09] installed kdesdk-umbrello (4.4.3-1)
[2010-05-28 16:09] installed kdetoys-amor (4.4.3-1)
[2010-05-28 16:09] installed kdetoys-kteatime (4.4.3-1)
[2010-05-28 16:09] installed kdetoys-ktux (4.4.3-1)
[2010-05-28 16:09] installed kdetoys-kweather (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-ark (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-kcalc (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-kcharselect (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-kdelirc (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-kdf (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-kfloppy (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-kgpg (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-ktimer (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-kwallet (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-okteta (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-printer-applet (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-superkaramba (4.4.3-1)
[2010-05-28 16:09] installed kdeutils-sweeper (4.4.3-1)
[2010-05-28 16:09] installed kdewebdev-kfilereplace (4.4.3-1)
[2010-05-28 16:09] installed kdewebdev-kimagemapeditor (4.4.3-1)
[2010-05-28 16:09] installed tidyhtml (1.46-1)
[2010-05-28 16:09] installed kdewebdev-klinkstatus (4.4.3-1)
[2010-05-28 16:09] installed kdewebdev-kommander (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-ar (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-bg (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-ca (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-ca@valencia (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-cs (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-csb (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-da (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-de (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-el (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-en_gb (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-eo (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-es (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-et (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-eu (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-fi (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-fr (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-fy (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-ga (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-gl (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-gu (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-he (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-hi (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-hr (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-hu (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-id (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-is (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-it (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-ja (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-kk (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-km (4.4.3-1)
```

```
[2010-05-28 16:09] installed kde-l10n-kn (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-ko (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-lt (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-lv (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-mai (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-mk (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-ml (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-nb (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-nds (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-nl (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-nn (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-pa (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-pl (4.4.3-1)
[2010-05-28 16:09] installed kde-l10n-pt (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-pt_br (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-ro (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-ru (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-si (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-sk (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-sl (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-sr (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-sv (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-tg (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-tr (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-uk (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-wa (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-zh_cn (4.4.3-1)
[2010-05-28 16:10] installed kde-l10n-zh_tw (4.4.3-1)
[2010-05-28 16:10] installed kde-meta-kdeaccessibility (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdeadmin (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdeartwork (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdebase (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdeedu (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdegames (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdegraphics (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdemultimedia (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdenetwork (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdepim (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdeplasma-addons (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdesdk (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdetoys (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdeutils (4.4-3)
[2010-05-28 16:10] installed kde-meta-kdewebdev (4.4-3)
[2010-05-28 16:10] installed qtcurve-gtk2 (1.4.1-1)
[2010-05-28 16:10] installed qt3 (3.3.8-17)
[2010-05-28 16:10] installed kdelibs3 (3.5.10-10)
[2010-05-28 16:10] installed qtcurve-kde3 (1.4.1-1)
[2010-05-28 16:10] installed qtcurve-kde4 (1.4.2-1)
[2010-05-28 16:10] installed compiz-core (0.8.6-2)
[2010-05-28 16:10] installed libcompizconfig (0.8.4-2)
[2010-05-28 16:10] installed pyrex (0.9.8.5-2)
[2010-05-28 16:10] installed compizconfig-python (0.8.4-1)
[2010-05-28 16:10] installed ccsm (0.8.4-1)
[2010-05-28 16:10] installed libcanberra (0.23-1)
[2010-05-28 16:10] installed zenity (2.30.0-1)
[2010-05-28 16:10] installed libgtop (2.28.1-1)
[2010-05-28 16:10] installed metacity (2.30.1-1)
[2010-05-28 16:10] installed libgnomekbd (2.30.1-1)
```

```
[2010-05-28 16:10] installed gnome-desktop (2.30.0-1)
[2010-05-28 16:10] installed gnome-settings-daemon (2.30.1-1)
[2010-05-28 16:10] installed sound-theme-freedesktop (0.7-1)
[2010-05-28 16:10] installed gnome-menus (2.30.0-1)
[2010-05-28 16:10] installed perlxml (2.36-2)
[2010-05-28 16:10] installed perl-xml-simple (2.18-2)
[2010-05-28 16:10] installed icon-naming-utils (0.8.90-1)
[2010-05-28 16:10] installed gnome-icon-theme (2.30.3-1)
[2010-05-28 16:10] installed libgweather (2.30.0-1)
[2010-05-28 16:10] installed evolution-data-server (2.30.1-1)
[2010-05-28 16:10] Unknown media type in type 'all/all'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'all/allfiles'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'uri/mms'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'uri/mmst'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'uri/mmsu'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'uri/pnm'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'uri/rtspt'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'uri/rtspu'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'fonts/package'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'interface/x-winamp-skin'
[2010-05-28 16:10]
[2010-05-28 16:10] installed gnome-control-center (2.30.1-1)
[2010-05-28 16:10] installed libxres (1.0.4-1)
[2010-05-28 16:10] installed libwnck (2.30.0-1)
[2010-05-28 16:10] installed compiz-decorator-gtk (0.8.6-2)
[2010-05-28 16:10] installed compiz-decorator-kde (0.8.6-2)
[2010-05-28 16:10] installed compiz-bcop (0.8.4-1)
[2010-05-28 16:10] installed compiz-fusion-plugins-main (0.8.6-1)
[2010-05-28 16:10] installed compiz-fusion-plugins-extra (0.8.6-1)
[2010-05-28 16:10] installed compizconfig-backend-gconf (0.8.4-1)
[2010-05-28 16:10] installed compizconfig-backend-kconfig (0.8.4-1)
[2010-05-28 16:10] Unknown media type in type 'all/all'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'all/allfiles'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'uri/mms'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'uri/mmst'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'uri/mmsu'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'uri/pnm'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'uri/rtspt'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'uri/rtspu'
[2010-05-28 16:10]
[2010-05-28 16:10] Unknown media type in type 'fonts/package'
[2010-05-28 16:10]
```

```
[2010-05-28 16:10] Unknown media type in type 'interface/x-winamp-skin'
[2010-05-28 16:10]
[2010-05-28 16:10] installed emerald (0.8.4-2)
[2010-05-28 16:10] installed emerald-themes (0.6.0-2)
[2010-05-28 16:10] > Updating icon cache.....
[2010-05-28 16:10] installed fusion-icon (20091023-1)
[2010-05-28 16:10] installed libwebkit (1.2.1-1)
[2010-05-28 16:10] installed gnome-js-common (0.1.2-1)
[2010-05-28 16:10] installed gobject-introspection (0.6.12-1)
[2010-05-28 16:10] installed seed (2.30.0-1)
[2010-05-28 16:10] installed epiphany (2.30.2-1)
[2010-05-28 16:10] installed gnome-panel (2.30.0-1)
[2010-05-28 16:10] warning: /etc/conf.d/cpufreq saved as /etc/conf.d/cpufreq.pacorig
[2010-05-28 16:10] installed cpufrequtils (007-1)
[2010-05-28 16:10] installed gnome-applets (2.30.0-1)
[2010-05-28 16:10] installed gnome-backgrounds (2.30.0-1)
[2010-05-28 16:10] installed gstreamer0.10-good (0.10.22-1)
[2010-05-28 16:10] installed libavc1394 (0.5.3-3)
[2010-05-28 16:10] installed libiec61883 (1.2.0-1)
[2010-05-28 16:10] installed speex (1.2rc1-1)
[2010-05-28 16:10] installed libshout (2.2.2-3)
[2010-05-28 16:10] installed libdv (1.0.0-3)
[2010-05-28 16:10] installed gstreamer0.10-good-plugins (0.10.22-1)
[2010-05-28 16:10] installed gnome-media (2.30.0-2)
[2010-05-28 16:10] installed gnome-screensaver (2.30.0-1)
[2010-05-28 16:10] installed upower (0.9.4-1)
[2010-05-28 16:10] installed polkit-gnome (0.96-3)
[2010-05-28 16:10] installed gnome-session (2.30.0-1)
[2010-05-28 16:10] installed gtk-engines (2.20.1-1)
[2010-05-28 16:10] installed gnome-themes (2.30.1-1)
[2010-05-28 16:10] installed docbook-xml (4.5-4)
[2010-05-28 16:10] installed gnome-doc-utils (0.20.1-1)
[2010-05-28 16:10] installed yelp (2.30.1-1)
[2010-05-28 16:11] installed gnome2-user-docs (2.30.0-1)
[2010-05-28 16:11] installed at-spi (1.30.1-1)
[2010-05-28 16:11] installed libgail-gnome (1.20.2-1)
[2010-05-28 16:11] installed exempi (2.1.1-1)
[2010-05-28 16:11] installed nautilus (2.30.1-1)
[2010-05-28 16:11] installed libsexy (0.1.11-2)
[2010-05-28 16:11] installed notification-daemon (0.4.0-4)
[2010-05-28 16:11] installed alacarte (0.13.1-1)
[2010-05-28 16:11] installed bug-buddy (2.30.0-1)
[2010-05-28 16:11] installed cheese (2.30.1-1)
[2010-05-28 16:11] installed gnome-speech (0.4.25-1)
[2010-05-28 16:11] installed dasher (4.10.1-2)
[2010-05-28 16:11] installed gnome-python-desktop (2.30.0-1)
[2010-05-28 16:11] installed deskbar-applet (2.30.1-1)
[2010-05-28 16:11] installed ptlib (2.6.5-2)
[2010-05-28 16:11] installed opal (3.6.6-2)
[2010-05-28 16:11] installed libsigc++2.0 (2.2.7-1)
[2010-05-28 16:11] installed ekiga (3.2.6-1)
[2010-05-28 16:11] installed telepathy-mission-control (5.4.2-1)
[2010-05-28 16:11] > To use Empathy you need to install at least one Telepathy connection
[2010-05-28 16:11] manager.
[2010-05-28 16:11] >
[2010-05-28 16:11] installed empathy (2.30.1-1)
[2010-05-28 16:11] installed eog (2.30.1-1)
[2010-05-28 16:11] installed poppler-glib (0.12.4-1)
```

```
[2010-05-28 16:11] installed t1lib (5.1.2-2)
[2010-05-28 16:11] installed evince (2.30.1-2)
[2010-05-28 16:11] installed gtkhtml (3.30.1-1)
[2010-05-28 16:11] warning: /etc/bluetooth/main.conf saved as /etc/bluetooth/main.conf.pacorig
[2010-05-28 16:11] warning: /etc/bluetooth/audio.conf saved as /etc/bluetooth/audio.conf.pacorig
[2010-05-28 16:11] installed bluez (4.65-1)
[2010-05-28 16:11] installed pilot-link (0.12.5-1)
[2010-05-28 16:11] installed gnome-pilot (2.0.17-2)
[2010-05-28 16:11] installed libpst (0.6.41-4)
[2010-05-28 16:11] installed libytnef (1.5-2)
[2010-05-28 16:11] installed gtkimageview (1.6.4-1)
[2010-05-28 16:11] installed evolution (2.30.1.2-1)
[2010-05-28 16:11] installed evolution-exchange (2.30.1-1)
[2010-05-28 16:11] installed evolution-webcal (2.28.1-1)
[2010-05-28 16:11] installed file-roller (2.30.1.1-1)
[2010-05-28 16:11] installed gcalctool (5.30.1-1)
[2010-05-28 16:11] installed gconf-editor (2.30.0-1)
[2010-05-28 16:11] installed gdm (2.30.2-2)
[2010-05-28 16:11] installed gnome-audio (2.22.0-1)
[2010-05-28 16:11] installed guile (1.8.7-2)
[2010-05-28 16:11] installed clutter (1.2.8-1)
[2010-05-28 16:11] installed clutter-gtk (0.10.2-2)
[2010-05-28 16:11] installed gir-repository (0.6.6-0.20100311)
[2010-05-28 16:11] installed gnome-games (2.30.1-1)
[2010-05-28 16:12] installed gnome-games-extra-data (2.30.0-1)
[2010-05-28 16:12] installed gnome-mag (0.16.1-1)
[2010-05-28 16:12] installed gnome-netstatus (2.28.1-1)
[2010-05-28 16:12] installed xinetd (2.3.14-5)
[2010-05-28 16:12] installed netkit-bsd-finger (0.17-5)
[2010-05-28 16:12] installed whois (5.0.4-1)
[2010-05-28 16:12] installed gnome-nettool (2.30.0-1)
[2010-05-28 16:12] installed gnome-power-manager (2.30.1-1)
[2010-05-28 16:12] installed libgksu (2.0.12-2)
[2010-05-28 16:12] installed glibmm (2.24.2-1)
[2010-05-28 16:12] installed cairomm (1.8.4-1)
[2010-05-28 16:12] installed pangomm (2.26.2-1)
[2010-05-28 16:12] installed gtkmm (2.20.3-1)
[2010-05-28 16:12] installed gnome-system-monitor (2.28.1-1)
[2010-05-28 16:12] installed gnome-terminal (2.30.1-1)
[2010-05-28 16:12] installed gnome-utils (2.30.0-1)
[2010-05-28 16:12] installed gok (2.30.0-1)
[2010-05-28 16:12] installed python-pysqlite (2.5.5-1)
[2010-05-28 16:12] installed pyxdg (0.19-1)
[2010-05-28 16:12] installed hamster-applet (2.30.1-1)
[2010-05-28 16:12] installed mousetweaks (2.30.1-1)
[2010-05-28 16:12] installed nautilus-sendto (2.28.4-1)
[2010-05-28 16:12] installed tcl (8.5.8-1)
[2010-05-28 16:12] installed brltty (4.1-3)
[2010-05-28 16:12] installed orca (2.30.1-1)
[2010-05-28 16:12] installed seahorse (2.30.1-1)
[2010-05-28 16:12] installed seahorse-plugins (2.30.1-1)
[2010-05-28 16:12] installed gmime (2.4.17-1)
[2010-05-28 16:12] installed totem-plparser (2.30.1-1)
[2010-05-28 16:12] installed libbeagle (0.3.9-1)
[2010-05-28 16:12] installed cdrkit (1.1.10-1)
[2010-05-28 16:12] installed cdrdao (1.2.3-4)
[2010-05-28 16:12] installed dvd+rw-tools (7.1-2)
[2010-05-28 16:12] installed brasero (2.30.1-1)
```

```
[2010-05-28 16:12] installed sound-juicer (2.28.2-1)
[2010-05-28 16:12] installed gtkspell (2.0.16-1)
[2010-05-28 16:12] installed libgdiplus (2.6.4-1)
[2010-05-28 16:12] installed mono (2.6.4-2)
[2010-05-28 16:12] installed ndesk-dbus (0.6.0-2)
[2010-05-28 16:12] installed ndesk-dbus-glib (0.4.1-2)
[2010-05-28 16:12] installed gtk-sharp-2 (2.12.10-1)
[2010-05-28 16:12] installed gnome-sharp (2.24.1-1)
[2010-05-28 16:12] installed mono-addins (0.4-4)
[2010-05-28 16:12] installed gnome-desktop-sharp (2.26.0-5)
[2010-05-28 16:12] Unknown media type in type 'all/all'
[2010-05-28 16:12]
[2010-05-28 16:12] Unknown media type in type 'all/allfiles'
[2010-05-28 16:12]
[2010-05-28 16:12] Unknown media type in type 'uri/mms'
[2010-05-28 16:12]
[2010-05-28 16:12] Unknown media type in type 'uri/mmst'
[2010-05-28 16:12]
[2010-05-28 16:12] Unknown media type in type 'uri/mmsu'
[2010-05-28 16:12]
[2010-05-28 16:12] Unknown media type in type 'uri/pnm'
[2010-05-28 16:12]
[2010-05-28 16:12] Unknown media type in type 'uri/rtspt'
[2010-05-28 16:12]
[2010-05-28 16:12] Unknown media type in type 'uri/rtspu'
[2010-05-28 16:12]
[2010-05-28 16:12] Unknown media type in type 'fonts/package'
[2010-05-28 16:12]
[2010-05-28 16:12] Unknown media type in type 'interface/x-winamp-skin'
[2010-05-28 16:12]
[2010-05-28 16:12] installed tomboy (1.2.1-1)
[2010-05-28 16:12] installed totem (2.30.2-1)
[2010-05-28 16:12] installed gtk-vnc (0.3.10-1)
[2010-05-28 16:12] installed vinagre (2.30.1-1)
[2010-05-28 16:12] installed vino (2.28.2-1)
[2010-05-28 16:12] installed xf86-video-vesa (2.3.0-1)
[2010-05-28 16:12] installed xorg-docs (1.5-1)
[2010-05-28 16:12] installed xorg-fonts-alias (1.0.2-1)
[2010-05-28 16:13] Updating font cache... done.
[2010-05-28 16:13] installed xorg-fonts-100dpi (1.0.1-3)
[2010-05-28 16:13] Updating font cache... done.
[2010-05-28 16:13] installed xorg-fonts-75dpi (1.0.1-3)
[2010-05-28 16:13] installed xorg-res-utils (1.0.3-3)
[2010-05-28 16:13] installed libpciaccess (0.11.0-1)
[2010-05-28 16:13] installed xcursor-themes (1.0.2-1)
[2010-05-28 16:13] installed fontcacheproto (0.1.3-1)
[2010-05-28 16:13] installed libxfontcache (1.0.5-1)
[2010-05-28 16:13] installed mcpp (2.7.2-2)
[2010-05-28 16:13] installed xorg-server-utils (7.5-3)
[2010-05-28 16:13] Updating font cache... done.
[2010-05-28 16:13] installed xorg-fonts-misc (1.0.1-1)
[2010-05-28 16:13] installed xbitmaps (1.1.0-1)
[2010-05-28 16:13] installed xf86-input-evdev (2.3.2-1)
[2010-05-28 16:13]
[2010-05-28 16:13]   Input device handling has changed since xorg-server 1.5.
[2010-05-28 16:13]   Please read http://wiki.archlinux.org/index.php/Xorg_input_hotplugging.
[2010-05-28 16:13]
[2010-05-28 16:13] installed xorg-server (1.7.6-3)
```

```
[2010-05-28 16:13] installed xorg-twm (1.0.4-3)
[2010-05-28 16:13] warning: /etc/X11/xinit/xinitrc saved as /etc/X11/xinit/xinitrc.pacorig
[2010-05-28 16:13] installed xorg-xinit (1.2.1-1)
[2010-05-28 16:13] installed xterm (258-2)
[2010-05-28 16:13] installed xf86-video-apm (1.2.2-2)
[2010-05-28 16:13] installed xf86-video-ark (0.7.2-1)
[2010-05-28 16:13] installed ati-dri (7.7.1-1)
[2010-05-28 16:13] installed xf86-video-ati (6.12.192-1)
[2010-05-28 16:13] installed xf86-video-chips (1.2.2-2)
[2010-05-28 16:13] installed xf86-video-cirrus (1.3.2-2)
[2010-05-28 16:13] installed xf86-video-dummy (0.3.2-2)
[2010-05-28 16:13] installed xf86-video-fbdev (0.4.1-2)
[2010-05-28 16:13] installed xf86-video-glint (1.2.4-2)
[2010-05-28 16:13] installed xf86-video-i128 (1.3.3-2)
[2010-05-28 16:13] installed xf86-video-i740 (1.3.2-2)
[2010-05-28 16:13] installed intel-dri (7.7.1-1)
[2010-05-28 16:13] installed xf86-video-intel (2.10.0-1)
[2010-05-28 16:13] installed mach64-dri (7.7.1-1)
[2010-05-28 16:13] installed xf86-video-mach64 (6.8.2-2)
[2010-05-28 16:13] installed mga-dri (7.7.1-1)
[2010-05-28 16:13] installed xf86-video-mga (1.4.11-2)
[2010-05-28 16:13] installed xf86-video-neomagic (1.2.4-3)
[2010-05-28 16:13] installed xf86-video-nv (2.1.17-1)
[2010-05-28 16:13] installed r128-dri (7.7.1-1)
[2010-05-28 16:13] installed xf86-video-r128 (6.8.1-2)
[2010-05-28 16:13] installed xf86-video-radeonhd (1.3.0-1)
[2010-05-28 16:13] installed xf86-video-rendition (4.2.3-1)
[2010-05-28 16:13] installed xf86-video-s3 (0.6.3-1)
[2010-05-28 16:13] installed xf86-video-s3virge (1.10.4-1)
[2010-05-28 16:13] installed savage-dri (7.7.1-1)
[2010-05-28 16:13] installed xf86-video-savage (2.3.1-2)
[2010-05-28 16:13] installed xf86-video-siliconmotion (1.7.3-2)
[2010-05-28 16:13] installed sis-dri (7.7.1-1)
[2010-05-28 16:13] installed xf86-video-sis (0.10.2-3)
[2010-05-28 16:13] installed xf86-video-sisusb (0.9.3-1)
[2010-05-28 16:13] installed tdfx-dri (7.7.1-1)
[2010-05-28 16:13] installed xf86-video-tdfx (1.4.3-2)
[2010-05-28 16:13] installed xf86-video-trident (1.3.3-3)
[2010-05-28 16:13] installed xf86-video-tseng (1.2.3-1)
[2010-05-28 16:13] installed xf86-video-v4l (0.2.0-4)
[2010-05-28 16:13] installed xf86-video-vmware (10.16.9-1)
[2010-05-28 16:13] installed xf86-video-voodoo (1.2.3-1)
[2010-05-28 16:13] installed xf86-input-acecad (1.4.0-1)
[2010-05-28 16:13] installed xf86-input-aiptek (1.3.0-1)
[2010-05-28 16:13] installed xf86-input-elographics (1.2.3-3)
[2010-05-28 16:13] installed xf86-input-fpit (1.3.0-3)
[2010-05-28 16:13] installed xf86-input-hyperpen (1.3.0-3)
[2010-05-28 16:13] installed xf86-input-joystick (1.5.0-1)
[2010-05-28 16:13] installed xf86-input-keyboard (1.4.0-1)
[2010-05-28 16:13] installed xf86-input-mouse (1.5.0-1)
[2010-05-28 16:13] installed xf86-input-mutouch (1.2.1-4)
[2010-05-28 16:13] installed xf86-input-penmount (1.4.1-1)
[2010-05-28 16:13] installed xf86-input-synaptics (1.2.1-1)
[2010-05-28 16:13] installed xf86-input-vmmouse (12.6.5-3)
[2010-05-28 16:13] installed xf86-input-void (1.3.0-1)
[2010-05-28 16:16] warning: directory permissions differ on etc/privoxy/
```

filesystem: 750 package: 770 [2010-05-28 16:16] warning: /etc/privoxy/default.action saved as

/etc/privoxy/default.action.pacorig [2010-05-28 16:16] warning: /etc/privoxy/default.filter saved as /etc/privoxy/default.filter.pacorig [2010-05-28 16:16] warning: /etc/privoxy/config saved as /etc/privoxy/config.pacorig [2010-05-28 16:16] warning: directory permissions differ on etc/privoxy/templates/

filesystem: 750 package: 770 [2010-05-28 16:16] installed privoxy (3.0.16-1) [2010-05-28 16:18] installed lynx (2.8.7-2) [2010-05-28 16:18] warning: /etc/lighttpd/lighttpd.conf saved as /etc/lighttpd/lighttpd.conf.pacorig [2010-05-28 16:18] installed lighttpd (1.4.26-3) [2010-05-28 16:18] upgraded mysql (5.1.46-2 -> 5.1.46-2) [2010-05-28 16:19] upgraded lua (5.1.4-4 -> 5.1.4-4) [2010-05-28 16:19] installed xine-ui (0.99.6-1) [2010-05-28 16:20] upgraded mplayer (31147-2 -> 31147-2) [2010-05-28 16:20] installed smplayer (0.6.9-2) [2010-05-28 16:20] installed mutagen (1.19-1) [2010-05-28 16:20] installed exaile (0.3.1.1-1) [2010-05-28 16:22] upgraded exaile (0.3.1.1-1 -> 0.3.1.1-1) [2010-05-28 16:25] installed gstreamer0.10-bad (0.10.18-5) [2010-05-28 16:25] installed libusb1 (1.0.8-1) [2010-05-28 16:25] installed libdc1394 (2.1.2-1) [2010-05-28 16:25] installed libmms (0.5-2) [2010-05-28 16:25] installed libcdaudio (0.99.12-4) [2010-05-28 16:25] installed mjpegtools (1.9.0-3) [2010-05-28 16:25] installed libdvdread (4.1.3-2) [2010-05-28 16:25] installed libdvdnav (4.1.3-2) [2010-05-28 16:25] installed libmodplug (0.8.8.1-1) [2010-05-28 16:25] installed ladspa (1.13-2) [2010-05-28 16:25] installed liblrdf (0.4.0-6) [2010-05-28 16:25] installed soundtouch (1.5.0-1) [2010-05-28 16:25] installed libass (0.9.9-1) [2010-05-28 16:25] installed gstreamer0.10-bad-plugins (0.10.18-5) [2010-05-28 16:25] installed gstreamer0.10-ffmpeg (0.10.10-1) [2010-05-28 16:25] installed gstreamer0.10-ugly (0.10.14-4) [2010-05-28 16:25] installed libmpeg2 (0.5.1-1) [2010-05-28 16:25] installed libsidplay (1.36.59-4) [2010-05-28 16:25] installed gstreamer0.10-ugly-plugins (0.10.14-4) [2010-05-28 16:59] upgraded qt3 (3.3.8-17 -> 3.3.8-17) [2010-05-28 16:59] upgraded qt (4.6.2-4 -> 4.6.2-4) [2010-05-28 18:33] installed gtk-qt-engine (1.1-2) [2010-05-28 18:33] Change /etc/conf.d/vde to your needs. [2010-05-28 18:33] vde config files should be placed in /etc/vde, sample files are provided. [2010-05-28 18:33] iptables and dhcpd sample files have been installed to '/usr/share/vde2'. [2010-05-28 18:33] Merge those examples, if needed to the according config files. [2010-05-28 18:33] installed vde2 (2.2.2-6) [2010-05-28 18:33] >>> PLEASE READ FOR KVM USAGE! [2010-05-28 18:33] >>> Load the correct KVM module, you will need a KVM capable CPU! [2010-05-28 18:33] >>> Add yourself to the group 'kvm'. [2010-05-28 18:33] >>> Use 'qemu -enable-kvm' to use KVM. [2010-05-28 18:33] [2010-05-28 18:33] installed qemu (0.12.4-1) [2010-05-28 18:33] installed qtemu (1.0.5-3) [2010-05-28 18:33] installed qtcreator (1.3.1-1) [2010-05-28 18:33] installed recordmydesktop (0.3.8.1-4) [2010-05-28 18:33] installed qt-recordmydesktop (0.3.8-1) [2010-05-28 18:33] installed qtpfsgui (1.9.3-5) [2010-05-28 18:33] installed kvirc (3.4.2-4) [2010-05-28 18:33] installed xchat (2.8.6-6) [2010-05-28 18:33] installed silc-toolkit (1.1.10-1) [2010-05-28 18:33] installed cyrus-sasl-plugins (2.1.23-2) [2010-05-28 18:33] installed libpurple (2.7.0-1) [2010-05-28 18:33] installed pidgin (2.7.0-1) [2010-05-28 18:33] installed perl-error (0.17016-1) [2010-05-28 18:33] installed git (1.7.1-1) [2010-05-28 18:33] installed qgit (2.3-2) [2010-05-28 18:33] installed avidemux-cli (2.5.3-1) [2010-05-28 18:33] installed avidemux-qt (2.5.3-1) [2010-05-28 18:33] installed noyau (2.1-2) [2010-05-28 18:33] [2010-05-28 18:33] The correct device mode and /dev device file will need to be set in [2010-05-28 18:33] /etc/conf.d/inputattach.conf before starting /etc/rc.d/inputattach [2010-05-28 18:33] [2010-05-28 18:33] installed inputattach (1.24-2) [2010-05-28 18:33] installed inotail (0.5-3) [2010-05-28 18:33] installed quota-tools (3.17-1) [2010-05-28 18:33] installed xsensors (0.60-2) [2010-05-28 18:33] installed ksensors (0.7.3-5) [2010-05-28 18:33] installed ruby-glib2 (0.19.3-1) [2010-05-28 18:33] installed ruby-atk (0.19.3-1) [2010-05-28 18:33] installed ruby-pango (0.19.3-2) [2010-05-28 18:33] installed ruby-gdkpixbuf2 (0.19.3-2) [2010-05-28 18:33] installed ruby-rcairo (1.8.0-2) [2010-05-28 18:33] installed ruby-gtk2 (0.19.3-1) [2010-05-28 18:33] installed glib (1.2.10-8.1) [2010-05-28 18:33] installed gtk (1.2.10-10) [2010-05-28 18:33] installed gtk-theme-switch2 (2.1.0-1) [2010-05-28 18:33] installed gtk-theme-switch (1.0.1-3) [2010-05-28 18:33] installed gtk-xfce-engine (2.6.0-1) [2010-05-28 18:33] installed imlib (1.9.15-9) [2010-05-28 18:33] installed gtk1-engines (0.12-2) [2010-05-28 18:33] installed glib-perl (1.222-1) [2010-05-28 18:33] installed cairo-perl (1.061-1) [2010-05-28 18:33] installed pango-perl (1.221-1) [2010-05-28 18:33] installed gtk2-perl (1.221-1) [2010-05-28 20:00] installed cmake (2.8.1-2) [2010-05-28 20:01] installed cabextract (1.2-2) [2010-05-28 20:01] extracting fonts... done. [2010-05-28 20:02] rebuilding font cache... done. [2010-05-28 20:02] installed ttf-ms-fonts (2.0-3) [2010-05-28 20:03] removed boost (1.41.0-1) [2010-05-28 20:30] installed freeimage (3.13.1-1) [2010-05-28 20:30] installed zziplib (0.13.58-2) [2010-05-28 21:11] installed openal (1.12.854-1) [2010-05-28 21:11] installed freealut (1.1.0-3) [2010-05-28 21:36] removed freeimage (3.13.1-1) [2010-05-28 22:14] installed strace (4.5.20-1) [2010-05-29 06:23] installed gdb (7.1-2) [2010-05-29 09:36] installed gnome-alsamixer (0.9.6-3) [2010-05-29 09:36] installed alsa-firmware (1.0.23-1) [2010-05-

29 13:20] NOTE: [2010-05-29 13:20] If you experience any problems after installing xsane [2010-05-29 13:20] it may help to remove the setup and preferences files [2010-05-29 13:20] of xsane: [2010-05-29 13:20] [2010-05-29 13:20] $ rm -rf ~/.sane/xsane [2010-05-29 13:20] [2010-05-29 13:20] installed xsane (0.997-2) [2010-05-29 13:28] installed gimmage (0.2.3-2) [2010-05-29 22:23] installed libgnomecups (0.2.3-7) [2010-05-29 22:23] installed libgnomeprint (2.18.7-2) [2010-05-29 22:23] installed libgnomeprintui (2.18.5-1) [2010-05-29 22:23] installed ghex (2.24.0-1) [2010-05-30 10:05] synchronizing package lists [2010-05-30 10:05] starting full system upgrade [2010-05-30 10:07] synchronizing package lists [2010-05-30 10:07] starting full system upgrade [2010-05-30 10:11] upgraded linux-api-headers (2.6.33.2-1 -> 2.6.34-1) [2010-05-30 10:11] warning: /etc/locale.gen installed as /etc/locale.gen.pacnew [2010-05-30 10:11] Generating locales... [2010-05-30 10:11] en_GB.UTF-8... done [2010-05-30 10:11] en_GB.ISO-8859-1... done [2010-05-30 10:11] Generation complete. [2010-05-30 10:11] upgraded glibc (2.11.1-3 -> 2.12-2) [2010-05-30 10:11] upgraded binutils (2.20.1-2 -> 2.20.1-3) [2010-05-30 10:11] upgraded gcc (4.5.0-2 -> 4.5.0-3) [2010-05-30 10:11] upgraded gcc-ada (4.5.0-2 -> 4.5.0-3) [2010-05-30 10:11] upgraded gcc-fortran (4.5.0-2 -> 4.5.0-3) [2010-05-30 10:11] upgraded gcc-libs (4.5.0-2 -> 4.5.0-3) [2010-05-30 10:11] upgraded gcc-objc (4.5.0-2 -> 4.5.0-3) [2010-05-30 10:11] upgraded libmysqlclient (5.1.46-2 -> 5.1.47-1) [2010-05-30 10:11] upgraded mysql-clients (5.1.46-2 -> 5.1.47-1) [2010-05-30 10:11] upgraded mysql (5.1.46-2 -> 5.1.47-1) [2010-05-30 10:11] Fixing gshadow file ... [2010-05-30 10:11] upgraded shadow (4.1.4.2-2 -> 4.1.4.2-3) [2010-05-30 10:11] upgraded tar (1.23-2 -> 1.23-3) [2010-05-30 10:11] upgraded udisks (1.0.1-1 -> 1.0.1-2) [2010-05-30 10:11] upgraded whois (5.0.4-1 -> 5.0.5-1) [2010-06-03 10:41] synchronizing package lists [2010-06-03 10:42] starting full system upgrade [2010-06-03 10:43] installed cvs (1.11.23-5) [2010-06-03 10:43] installed libnet (1.1.4-1) [2010-06-03 10:43] installed ettercap (NG_0.7.3-15) [2010-06-03 10:43] installed ettercap-gtk (NG_0.7.3-7) [2010-06-03 10:43] installed libnids (1.24-1) [2010-06-03 10:43] installed dsniff (2.4b1-17) [2010-06-03 10:51] synchronizing package lists [2010-06-03 10:52] installed kdebindings-smoke (4.4.4-1) [2010-06-03 10:52] installed kdebindings-ruby (4.4.4-1) [2010-06-03 10:52] installed mysql-ruby (2.8.1-2) [2010-06-03 10:52] installed ruby-docs (1.9.1_p378-2) [2010-06-03 10:52] installed ruby-gconf2 (0.19.3-2) [2010-06-03 10:52] installed ruby-locale (2.0.5-1) [2010-06-03 10:52] installed ruby-gettext (2.1.0-1) [2010-06-03 10:52] installed ruby-libart (0.19.3-2) [2010-06-03 10:52] installed ruby-gnomecanvas (0.19.3-3.1) [2010-06-03 10:52] installed ruby-gnome2 (0.19.4-1) [2010-06-03 10:52] installed ruby-hpricot (0.8.2-1) [2010-06-03 10:52] installed ruby-libglade (0.19.3-1) [2010-06-03 10:52] installed ruby-mpd (0.2.3-1) [2010-06-03 10:52] installed ruby-ncurses (1.2.4-1) [2010-06-03 10:52] installed ruby-sqlite3 (1.2.4-2) [2010-06-03 10:52] warning: /etc/vimrc saved as /etc/vimrc.pacorig [2010-06-03 10:52] installed vim-runtime (7.2-1) [2010-06-03 10:52] installed vim (7.2-1) [2010-06-03 10:52] updating Vim help tags... done. [2010-06-03 10:52] installed vim-rails (4.2-1) [2010-06-03 11:06] synchronizing package lists [2010-06-03 11:07] starting full system upgrade [2010-06-03 12:43] starting full system upgrade [2010-06-03 14:50] starting full system upgrade [2010-06-04 08:27] upgraded gcc (4.5.0-3 -> 4.5.0-4) [2010-06-04 08:27] upgraded gcc-libs (4.5.0-3 -> 4.5.0-4) [2010-06-04 08:27] upgraded gcc-ada (4.5.0-3 -> 4.5.0-4) [2010-06-04 08:27] upgraded gcc-objc (4.5.0-3 -> 4.5.0-4) [2010-06-04 08:27] upgraded gcc-fortran (4.5.0-3 -> 4.5.0-4) [2010-06-05 08:49] installed macchanger (1.5.0-3) [2010-06-07 15:19] installed k3b (1.92.0rc3-1) [2010-06-07 15:21] installed vcdimager (0.7.23-7) [2010-06-07 15:21] installed imagemagick (6.6.2.0-1) [2010-06-07 15:21] installed transcode (1.1.5-3) [2010-06-07 15:21] installed emovix (0.9.0-4) [2010-06-08 08:51] installed dia (0.97-3) [2010-06-11 07:03] synchronizing package lists [2010-06-11 07:07] upgraded thunderbird (3.0.4-1 -> 3.0.4-1) [2010-06-11 07:10] upgraded pango (1.28.0-1 -> 1.28.0-1) [2010-06-11 07:10] upgraded pangomm (2.26.2-1 -> 2.26.2-1) [2010-06-11 08:19] installed zip (3.0-1) [2010-06-11 08:19] upgraded unzip (6.0-5 -> 6.0-5) [2010-06-13 09:15] synchronizing package lists [2010-06-13 09:17] installed qca-gnupg (2.0.0-1) [2010-06-13 09:17] installed psi (0.14-3) [2010-06-13 12:00] installed wxgtk (2.8.11-1) [2010-06-13 12:00] installed filezilla (3.3.2.1-1) [2010-06-13 12:44] upgraded libpurple (2.7.0-1 -> 2.7.1-1) [2010-06-13 12:44] upgraded pidgin (2.7.0-1 -> 2.7.1-1) [2010-06-16 09:09] synchronizing package lists [2010-06-25 11:48] installed printproto (1.0.4-2) [2010-06-25 11:48] installed libxp (1.0.0-3) [2010-06-25 11:48] installed lesstif (0.95.2-2) [2010-06-25 11:48] installed xpdf (3.02_pl4-2) [2010-06-25 11:53] upgraded silc-toolkit (1.1.10-1 -> 1.1.10-1) [2010-06-25 12:44] installed giblib (1.2.4-4) [2010-06-25 12:44] installed scrot (0.8-4) [2010-06-26 14:27] synchronizing package lists [2010-06-26 14:28] warning: /etc/pacman.conf installed as /etc/pacman.conf.pacnew [2010-06-26 14:28] warning: /etc/makepkg.conf installed as /etc/makepkg.conf.pacnew [2010-06-26 14:28] upgraded pacman (3.3.3-5 -> 3.4.0-2) [2010-06-26 14:28] Running 'pacman -S –noconfirm xfce4' [2010-06-26 14:29] upgraded gtk-xfce-engine (2.6.0-1 -> 2.6.0-1) [2010-06-26 14:29] installed libxfce4util (4.6.2-1) [2010-06-26 14:29] installed xfconf (4.6.2-1) [2010-06-26 14:29] installed libxfcegui4 (4.6.4-1) [2010-06-26 14:29]

installed mousepad (0.2.16-2) [2010-06-26 14:29] installed exo (0.3.107-1) [2010-06-26 14:29] installed xfce4-panel (4.6.4-1) [2010-06-26 14:29] installed orage (4.6.1-1) [2010-06-26 14:29] installed terminal (0.4.5-1) [2010-06-26 14:29] installed thunar (1.0.2-1) [2010-06-26 14:29] NOTE [2010-06-26 14:29] —- [2010-06-26 14:29] > xfce can run on top of a framebuffer. However, for most users it is [2010-06-26 14:29] > best to install xorg as an x-server. Please install either xorg-xinit [2010-06-26 14:29] > as minimal environment or the xorg meta package. [2010-06-26 14:29] pacman -S xorg-xinit [2010-06-26 14:29] – or – [2010-06-26 14:29] pacman -S xorg [2010-06-26 14:29] installed xfce-utils (4.6.2-1) [2010-06-26 14:29] installed libxfce4menu (4.6.2-1) [2010-06-26 14:29] installed xfce4-appfinder (4.6.2-1) [2010-06-26 14:29] installed xfce4-mixer (4.6.1-1) [2010-06-26 14:29] installed xfce4-session (4.6.2-1) [2010-06-26 14:29] installed tango-icon-theme (0.8.90-2) [2010-06-26 14:29] installed xfce4-settings (4.6.5-1) [2010-06-26 14:30] installed xfdesktop (4.6.2-1) [2010-06-26 14:30] installed psutils (1.17-2) [2010-06-26 14:30] installed a2ps (4.14-1) [2010-06-26 14:30] installed xfprint (4.6.1-3) [2010-06-26 14:30] installed xfwm4 (4.6.2-1) [2010-06-26 14:30] installed xfwm4-themes (4.6.0-1) [2010-06-26 16:36] Running ‘pacman -Sy’ [2010-06-26 16:36] synchronizing package lists [2010-06-26 16:38] Running ‘pacman -Scc’

Log Samples for rshd

```
Dec 17 10:49:23 hostname rshd[347339]: Connection from 10.217.223.31 on illegal port
```

I enabled SELinux on my Kubuntu workstation and almost immediately received notifications from OSSEC. It has been a while since I reviewed the [http://www.centos.org/docs/4/html/rhel-selg-en-4/ RHEL SELinux documentation] that explains these log entries from /var/log/messages. There’s a very real possibility that I did not set SELinux up properly, it is not very well supported by Ubuntu at the moment. I may change this entry after I re-review the SELinux docs.

Anyway, here’s something to chew on FWIW ...

```
Feb 20 16:57:43 localhost kernel: [17180270.076000] audit(1172015863.889:2): avc:  denied  { append
Feb 20 16:57:43 localhost kernel: [17180270.076000] audit(1172015863.889:3): avc:  denied  { write }
Feb 20 16:57:43 localhost kernel: [17180270.076000] audit(1172015863.889:4): avc:  denied  { read } i
Feb 20 16:57:43 localhost kernel: [17180270.100000] audit(1172015863.913:5): avc:  denied  { write }
Feb 20 16:57:43 localhost kernel: [17180270.100000] audit(1172015863.913:6): avc:  denied  { read } i
Feb 20 16:57:43 localhost kernel: [17180270.128000] inode_doinit_with_dentry:  no dentry for dev=sda
Feb 20 16:57:44 localhost kernel: [17180270.404000] audit(1172015864.217:7): avc:  denied  { read } i
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:9): avc:  denied  { write }
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:10): avc:  denied  { read }
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:11): avc:  denied  { syslog_
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:12): avc:  denied  { append
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:13): avc:  denied  { write
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:14): avc:  denied  { read }
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:15): avc:  denied  { read }
Feb 20 16:57:44 localhost kernel: [17180270.428000] audit(1172015864.241:16): avc:  denied  { read }
Feb 20 16:57:44 localhost kernel: [17180270.428000] audit(1172015864.241:17): avc:  denied  { create
Feb 20 16:57:44 localhost kernel: [17180270.432000] audit(1172015864.245:18): avc:  denied  { write
Feb 20 16:57:44 localhost kernel: [17180270.536000] audit(1172015864.349:19): avc:  denied  { search
Feb 20 16:57:44 localhost kernel: [17180270.536000] audit(1172015864.349:20): avc:  denied  { read }
Feb 20 16:57:44 localhost kernel: [17180270.540000] audit(1172015864.353:21): avc:  denied  { ioctl
Feb 20 16:57:44 localhost kernel: [17180270.600000] audit(1172015864.413:22): avc:  denied  { write
Feb 20 16:57:44 localhost kernel: [17180270.600000] audit(1172015864.413:23): avc:  denied  { read }
Feb 20 16:57:44 localhost kernel: [17180270.600000] audit(1172015864.413:24): avc:  denied  { write
Feb 20 16:57:44 localhost kernel: [17180270.984000] audit(1172015864.797:25): avc:  denied  { rename
Feb 20 16:57:43 localhost kernel: [17180270.076000] audit(1172015863.889:2): avc:  denied  { append
Feb 20 16:57:43 localhost kernel: [17180270.076000] audit(1172015863.889:3): avc:  denied  { write }
Feb 20 16:57:43 localhost kernel: [17180270.076000] audit(1172015863.889:4): avc:  denied  { read } i
Feb 20 16:57:43 localhost kernel: [17180270.100000] audit(1172015863.913:5): avc:  denied  { write }
```

```
Feb 20 16:57:43 localhost kernel: [17180270.100000] audit(1172015863.913:6): avc:  denied  { read } f
Feb 20 16:57:44 localhost kernel: [17180270.404000] audit(1172015864.217:7): avc:  denied  { read } f
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:9): avc:  denied  { write }
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:10): avc:  denied  { read }
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:11): avc:  denied  { syslog_
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:12): avc:  denied  { append
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:13): avc:  denied  { write
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:14): avc:  denied  { read }
Feb 20 16:57:44 localhost kernel: [17180270.424000] audit(1172015864.237:15): avc:  denied  { read }
Feb 20 16:57:44 localhost kernel: [17180270.428000] audit(1172015864.241:16): avc:  denied  { read }
Feb 20 16:57:44 localhost kernel: [17180270.428000] audit(1172015864.241:17): avc:  denied  { create
Feb 20 16:57:44 localhost kernel: [17180270.432000] audit(1172015864.245:18): avc:  denied  { write
Feb 20 16:57:44 localhost kernel: [17180270.536000] audit(1172015864.349:19): avc:  denied  { search
Feb 20 16:57:44 localhost kernel: [17180270.536000] audit(1172015864.349:20): avc:  denied  { read }
Feb 20 16:57:44 localhost kernel: [17180270.540000] audit(1172015864.353:21): avc:  denied  { ioctl
Feb 20 16:57:44 localhost kernel: [17180270.600000] audit(1172015864.413:22): avc:  denied  { write
Feb 20 16:57:44 localhost kernel: [17180270.600000] audit(1172015864.413:23): avc:  denied  { read }
Feb 20 16:57:44 localhost kernel: [17180270.600000] audit(1172015864.413:24): avc:  denied  { write
Feb 20 16:57:44 localhost kernel: [17180270.984000] audit(1172015864.797:25): avc:  denied  { rename
Feb 20 16:57:45 localhost kernel: [17180271.728000] audit(1172015865.541:26): avc:  denied  { unlink
Feb 20 16:57:45 localhost kernel: [17180271.728000] audit(1172015865.541:27): avc:  denied  { link }
Feb 20 16:57:45 localhost kernel: [17180272.040000] audit(1172015865.853:28): avc:  denied  { getattr
Feb 20 16:57:45 localhost kernel: [17180272.040000] audit(1172015865.853:29): avc:  denied  { read }
Feb 20 16:57:46 localhost kernel: [17180272.808000] audit(1172015866.621:30): avc:  denied  { read }
Feb 20 16:57:46 localhost kernel: [17180272.948000] audit(1172015866.761:31): avc:  denied  { write
Feb 20 16:57:46 localhost kernel: [17180272.948000] audit(1172015866.761:32): avc:  denied  { ioctl
Feb 20 16:57:45 localhost kernel: [17180271.728000] audit(1172015865.541:26): avc:  denied  { unlink
Feb 20 16:57:45 localhost kernel: [17180271.728000] audit(1172015865.541:27): avc:  denied  { link }
Feb 20 16:57:45 localhost kernel: [17180272.040000] audit(1172015865.853:28): avc:  denied  { getattr
Feb 20 16:57:45 localhost kernel: [17180272.040000] audit(1172015865.853:29): avc:  denied  { read }
Feb 20 16:57:46 localhost kernel: [17180272.808000] audit(1172015866.621:30): avc:  denied  { read }
Feb 20 16:57:46 localhost kernel: [17180272.948000] audit(1172015866.761:31): avc:  denied  { write
Feb 20 16:57:46 localhost kernel: [17180272.948000] audit(1172015866.761:32): avc:  denied  { ioctl
Feb 20 16:57:47 localhost kernel: [17180273.536000] audit(1172015867.349:33): avc:  denied  { search
Feb 20 16:57:47 localhost kernel: [17180273.560000] audit(1172015867.373:34): avc:  denied  { setattr
Feb 20 16:57:48 localhost kernel: [17180274.768000] audit(1172015868.581:35): avc:  denied  { read }
Feb 20 16:57:48 localhost kernel: [17180274.768000] audit(1172015868.581:36): avc:  denied  { getattr
Feb 20 16:57:47 localhost kernel: [17180273.536000] audit(1172015867.349:33): avc:  denied  { search
Feb 20 16:57:47 localhost kernel: [17180273.560000] audit(1172015867.373:34): avc:  denied  { setattr
Feb 20 16:57:48 localhost kernel: [17180274.768000] audit(1172015868.581:35): avc:  denied  { read }
Feb 20 16:57:48 localhost kernel: [17180274.768000] audit(1172015868.581:36): avc:  denied  { getattr
```

Log Samples from S.M.A.R.T

smartd example:

```
Jun 16 18:34:31 Lab8 smartd[2842]: Device: /dev/sda [SAT], SMART Usage Attribute: 194 Temperature_Cel
Jun 16 18:54:31 Lab8 -- MARK --
Jun 16 19:04:31 Lab8 smartd[2842]: Device: /dev/sda [SAT], SMART Prefailure Attribute: 7 Seek_Error_R
Jun 16 12:32:40 Lab9 smartd[2881]: Configuration file /etc/smartd.conf was parsed, found DEVICESCAN,
Jun 16 12:32:40 Lab9 smartd[2881]: Device: /dev/sda, type changed from 'scsi' to 'sat'
Jun 16 12:32:40 Lab9 smartd[2881]: Device: /dev/sda [SAT], opened
Jun 16 12:32:40 Lab9 smartd[2881]: Device: /dev/sda [SAT], found in smartd database.
Jun 16 12:32:40 Lab9 smartd[2881]: Device: /dev/sda [SAT], is SMART capable. Adding to "monitor" list
Jun 16 12:32:40 Lab9 smartd[2881]: Device: /dev/sda [SAT], state read from /var/lib/smartmontools/sma
Jun 16 12:32:40 Lab9 smartd[2881]: Monitoring 1 ATA and 0 SCSI devices
Jun 16 12:32:40 Lab9 smartd[2881]: Device: /dev/sda [SAT], 1 Currently unreadable (pending) sectors
```

```
Jun 16 12:32:40 Lab9 smartd[2881]: Device: /dev/sda [SAT], 1 Offline uncorrectable sectors
Jun 16 12:32:40 Lab9 smartd[2881]: Device: /dev/sda [SAT], SMART Prefailure Attribute: 1 Raw_Read_Err
Jun 16 12:32:40 Lab9 smartd[2881]: Device: /dev/sda [SAT], SMART Usage Attribute: 190 Airflow_Tempera
Jun 16 12:32:40 Lab9 smartd[2881]: Device: /dev/sda [SAT], SMART Usage Attribute: 194 Temperature_Cel
Jun 16 12:32:40 Lab9 smartd[2881]: Device: /dev/sda [SAT], SMART Usage Attribute: 195 Hardware_ECC_Re
Jun 16 12:32:40 Lab9 smartd[2881]: Device: /dev/sda [SAT], state written to /var/lib/smartmontools/sm
Jun 16 12:32:40 Lab9 smartd[2987]: smartd has fork()ed into background mode. New PID=2987.
```

Log samples for syslogd

Syslogd on OpenBSD (exiting and restarting):

```
Dec 19 20:00:01 enigma syslogd: restart
Dec 20 01:00:01 enigma syslogd: restart
Dec 20 14:29:41 enigma syslogd: exiting on signal 15
```

Syslogd on Ubuntu (exiting and restarting):

```
Dec 19 07:35:21 localhost exiting on signal 15
Dec 19 16:49:31 localhost syslogd 1.4.1#17ubuntu3: restart.
```

Log samples for errors on xfs partitions:

```
Jun  8 13:39:55 www kernel:  <1>XFS internal error XFS_WANT_CORRUPTED_RETURN at line 295 of file fs/x
Jun  8 13:39:55 www kernel: XFS internal error XFS_WANT_CORRUPTED_RETURN at line 295 of file fs/xfs/x
Jun  8 13:39:55 www kernel: XFS internal error XFS_WANT_CORRUPTED_RETURN at line 295 of file fs/xfs/x
Jun  8 13:39:55 www kernel: XFS internal error XFS_WANT_CORRUPTED_RETURN at line 295 of file fs/xfs/x
Jun  8 13:39:55 www kernel: XFS internal error XFS_WANT_CORRUPTED_RETURN at line 295 of file fs/xfs/x
Jun  9 14:04:32 www kernel:  <1>XFS internal error XFS_WANT_CORRUPTED_RETURN at line 295 of file fs/x
Jun  9 14:04:32 www kernel: XFS internal error XFS_WANT_CORRUPTED_RETURN at line 295 of file fs/xfs/x
```

Yum log samples

```
Dec  7 07:05:06 ax yum: Installed: libX11-devel - 1.0.3-9.el5.i386
Dec  7 07:05:06 ax yum: Installed: libXext-devel - 1.0.1-2.1.i386
Dec  7 07:05:07 ax yum: Installed: libICE-devel - 1.0.1-2.1.i386
Dec  7 14:03:48 axz yum-updatesd-helper: error getting update info: Cannot retrieve repository metada
Dec 18 01:50:16 xyz yum: Updated: nspr - 4.7.3-2.el5.x86_64
Dec 18 01:50:16 xyz yum: Updated: nss - 3.12.2.0-2.el5.x86_64
Aug 20 12:45:56 Updated: perl.i386 4:5.8.8-10.el5_2.3
Aug 20 12:46:57 Installed: device-mapper-event.i386 1.02.24-1.el5
Aug 20 12:51:21 Erased: libhugetlbfs-lib
```

Windows Logs

IIS Logs

Psoft H-Sphere IIS Log File Format

1. Software: Psoft H-Sphere running on Microsoft Internet Information Services 6.0
2. Version: 1.0

3. Date: 2007-03-04
4. Fields: date time c-ip cs-username s-sitename s-computername s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status sc-win32-status sc-bytes cs-bytes time-taken cs-version cs(User-Agent) cs(Cookie) cs(Referer)

IIS Logs saved on E:hslogfileswwwW3SVC*ex%y%m%d.log (where W3SVC* is sites 1-254 and ex070304.log):

```
#Software: H-Sphere log plugin
#Date: 2007-03-03 01:17:39
#Fields: date time c-ip cs-username s-sitename s-computername s-ip s-port cs-method cs-uri-stem cs-ur
2007-03-03 01:17:39 66.194.6.79 - W3SVC3 SERVER55 192.168.1.15 80 GET /index.html - 200 0 17691 117 1
2007-03-03 10:23:40 24.252.248.163 - W3SVC3 SERVER55 192.168.1.15 80 GET /images/9a.jpg - 200 0 32022
```

W3C Extended Log File Format

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2006-08-13 00:00:35
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-
2006-08-13 00:00:35 10.3.4.2 GET /iisstart.htm - 80 - 10.3.0.5 check_http/1.7+(nagios-plugins+) 200 0
2006-08-13 00:00:56 10.3.4.2 GET /iisstart.htm - 80 - 10.3.3.11 - 200 0 0
2006-08-13 00:01:44 10.3.4.2 GET /iisstart.htm - 80 - 10.3.0.5 check_http/1.7+(nagios-plugins+) 200 0
```

Log Samples from BSD systems

OpenBSD file system full:

```
Dec 30 21:01:13 bsd1 /bsd: uid 0 on /: file system full
Dec 30 21:07:01 bsd1 /bsd: uid 0 on /tmp: file system full
Dec 30 21:09:25 bsd1 pflogd[1234]: Logging suspended: fwrite: No space left
```

FreeBSD authentication failures:

```
Jan  9 14:00:28 t123 login: pam_ldap: error trying to bind as user "uid=xx,ou=Users,dc=yy,dc=zz,dc=co
Jan  9 14:00:37 t123 login: pam_ldap: error trying to bind as user "uid=xx,ou=Users,dc=yy,dc=zz,dc=co
Jan  9 14:00:41 t123 login: 2 LOGIN FAILURES FROM xx.yy.net.pl
```

FreeBSD NTP sync messages:

```
Jan  9 18:00:11 t123 ntpdate[92110]: adjust time server 1.2.3.4 offset 0.053179 sec
Jan  9 19:00:04 t123 ntpdate[92238]: adjust time server 1.2.3.4 offset 0.095983 sec
Jan  9 20:00:04 t123 ntpdate[92364]: adjust time server 1.2.3.4 offset 0.048435 sec
```

Log entries in asl.log on OSX

Note: user's name changed to "username" and host's name changed to "Hostname" to protect the innocent.

Sudo:

```
[Time 2006.12.28 15:54:03 UTC] [Facility local2] [Sender sudo] [PID -1] [Message   username : TTY=tty
[Time 2006.12.23 22:10:45 UTC] [Facility local2] [Sender sudo] [PID -1] [Message   username : TTY=tty
[Time 2006.12.23 22:11:19 UTC] [Facility local2] [Sender sudo] [PID -1] [Message   username : TTY=tty
[Time 2006.12.23 22:11:30 UTC] [Facility local2] [Sender sudo] [PID -1] [Message   username : TTY=tty
```

sshd:

```
[Time 2006.12.28 15:53:55 UTC] [Facility auth] [Sender sshd] [PID 483] [Message error: PAM: Authentic
[Time 2006.11.02 11:41:44 UTC] [Facility auth] [Sender sshd] [PID 800] [Message refused connect from
```

Cron:

```
[Time 2006.12.28 14:15:00 UTC] [Facility cron] [Sender anacron] [PID 459] [Message Updated timestamp
[Time 2006.12.28 14:18:00 UTC] [Facility cron] [Sender anacron] [PID 455] [Message Job `cron.daily' t
[Time 2006.12.28 14:18:00 UTC] [Facility cron] [Sender anacron] [PID 455] [Message Normal exit (1 job
[Time 2006.12.28 15:10:00 UTC] [Facility cron] [Sender anacron] [PID 481] [Message Anacron 2.3 starte
[Time 2006.12.28 15:10:00 UTC] [Facility cron] [Sender anacron] [PID 481] [Message Normal exit (0 job
```

Software Update:

```
[Time 2006.12.28 01:59:49 UTC] [Facility install] [Sender Software Update] [PID 353] [Message JavaScr
[Time 2006.12.28 01:59:49 UTC] [Facility install] [Sender Software Update] [PID 353] [Message __choic
[Time 2006.12.28 01:59:52 UTC] [Facility install] [Sender Software Update] [PID 353] [Message Package
[Time 2006.12.28 01:59:52 UTC] [Facility install] [Sender Software Update] [PID 353] [Message Package
[Time 2006.12.28 01:59:52 UTC] [Facility install] [Sender Software Update] [PID 353] [Message Package
[Time 2006.12.28 01:59:55 UTC] [Facility install] [Sender Software Update] [PID 353] [Message JavaScr
[Time 2006.12.28 01:59:55 UTC] [Facility install] [Sender Software Update] [PID 353] [Message __choic
```

Postfix:

```
[Time 2006.12.24 17:15:01 UTC] [Facility mail] [Sender postfix/postqueue] [PID 265] [Message warning:
```

Configd:

```
[Time 2006.12.23 17:44:48 UTC] [Facility daemon] [Sender configd] [PID 40] [Message AppleTalk shutdow
[Time 2006.12.23 17:44:48 UTC] [Facility daemon] [Sender configd] [PID 40] [Message AppleTalk shutdow
[Time 2006.12.23 17:44:52 UTC] [Facility daemon] [Sender configd] [PID 40] [Message posting notificat
```

Crashdump:

```
[Time 2006.12.23 17:30:23 UTC] [Facility daemon] [Sender crashdump] [PID 5546] [Message dummy-5507 cr
[Time 2006.12.23 17:30:23 UTC] [Facility daemon] [Sender crashdump] [PID 5546] [Message crash report
```

Launchd:

```
[Time 2006.12.23 17:20:00 UTC] [Facility launchd] [Sender launchd] [PID -1] [Message Server 0 in boot
[Time 2006.12.23 17:20:00 UTC] [Facility daemon] [Sender configd] [PID 40] [Message AppleTalk startup
[Time 2006.12.23 17:20:01 UTC] [Facility netinfo] [Sender lookupd] [PID 3126] [Message lookupd (versi
[Time 2006.12.23 17:20:03 UTC] [Facility launchd] [Sender launchd] [PID -1] [Message Server 0 in boot
```

OS X IPFW Log Samples

```
Aug 21 21:37:18 Macinfish ipfw:  12190 Deny TCP 83.227.141.74:4835 192.168.11.111:6881 in via en1
Aug 21 21:37:27 Macinfish ipfw:  12190 Deny TCP 83.227.141.74:4835 192.168.11.111:6881 in via en1
Aug 25 10:32:19 Macinfish ipfw:  12190 Deny TCP 192.168.11.123:64748 10.10.10.13:4444 in via en0
Aug 27 14:32:58 Macinfish ipfw:  12190 Deny TCP 192.168.13.1:2060 192.168.13.104:5000 in via en1
Aug 27 14:33:01 Macinfish ipfw:  12190 Deny TCP 192.168.13.1:2060 192.168.13.104:5000 in via en1
Aug 27 14:33:07 Macinfish ipfw:  12190 Deny TCP 192.168.13.1:2060 192.168.13.104:5000 in via en1
Aug 27 14:33:19 Macinfish ipfw:  12190 Deny TCP 192.168.13.1:2060 192.168.13.104:5000 in via en1
Aug 27 14:33:43 Macinfish ipfw:  12190 Deny TCP 192.168.13.1:2060 192.168.13.104:5000 in via en1
Aug 29 10:36:44 Macinfish ipfw:  12190 Deny TCP 192.168.10.2:10000 192.168.11.122:23 in via en0
Aug 29 10:36:44 Macinfish ipfw:  12190 Deny TCP 192.168.10.2:10000 192.168.11.122:80 in via en0
Aug 29 10:36:44 Macinfish ipfw:  12190 Deny TCP 192.168.10.2:10000 192.168.11.122:443 in via en0
Aug 29 10:36:44 Macinfish ipfw:  12190 Deny TCP 192.168.10.2:10000 192.168.11.122:137 in via en0
Aug 29 10:36:44 Macinfish ipfw:  12190 Deny TCP 192.168.10.2:10000 192.168.11.122:138 in via en0
Aug 29 10:36:44 Macinfish ipfw:  12190 Deny TCP 192.168.10.2:10000 192.168.11.122:139 in via en0
Aug 29 10:36:44 Macinfish ipfw:  12190 Deny TCP 192.168.10.2:10000 192.168.11.122:445 in via en0
Aug 29 10:36:44 Macinfish ipfw:  12190 Deny TCP 192.168.10.2:10000 192.168.11.122:20 in via en0
Aug 29 10:36:44 Macinfish ipfw:  12190 Deny TCP 192.168.10.2:10000 192.168.11.122:25 in via en0
```

Log samples Mac

Authentication failure:

```
Aug 11 17:22:14 hocha com.apple.SecurityServer: authinternal failed to authenticate user root.
Aug 11 17:22:14 hocha com.apple.SecurityServer: Failed to authorize right system.login.tty by process
Aug 11 17:22:16 hocha com.apple.SecurityServer: authinternal failed to authenticate user root.
Aug 11 17:22:16 hocha com.apple.SecurityServer: Failed to authorize right system.login.tty by process
Aug 11 17:22:17 hocha com.apple.SecurityServer: authinternal failed to authenticate user root.
Aug 11 17:22:17 hocha com.apple.SecurityServer: Failed to authorize right system.login.tty by process
```

FTP Logs

Microsoft FTPD examples

Sample 1:

```
14:03:19 192.168.2.187 [62]USER Administrator 331 0
14:03:19 192.168.2.187 [62]PASS - 530 1326
14:03:19 192.168.2.187 [62]USER Administrator 331 0
14:03:19 192.168.2.187 [62]PASS - 530 1326
14:03:19 192.168.2.187 [62]USER Administrator 331 0
14:03:20 192.168.2.187 [62]PASS - 530 1326
14:03:20 192.168.2.187 [62]USER Administrator 331 0
14:03:20 192.168.2.187 [62]PASS - 530 1326
14:03:20 192.168.2.187 [62]USER Administrator 331 0
```

```
14:03:20 192.168.2.187 [62]PASS - 530 1326
14:03:21 192.168.2.187 [62]USER Administrator 331 0
14:03:21 192.168.2.187 [62]PASS - 530 1326
14:37:52 10.1.2.35 [63]USER username 331 0
14:37:52 10.1.2.35 [63]PASS - 230 0
14:37:52 10.1.2.35 [63]CWD /dir 250 0
14:37:52 10.1.2.35 [63]CWD /dir/_mm 550 2
14:37:52 10.1.2.35 [63]CWD /dir/_notes 250 0
14:37:54 10.1.2.35 [63]CWD / 250 0
14:37:54 10.1.2.35 [63]MKD /dir/XYIZNWSK 257 0
14:37:54 10.1.2.35 [63]CWD /dir 250 0
14:37:54 10.1.2.35 [63]CWD / 250 0
14:37:54 10.1.2.35 [63]RMD /dir/XYIZNWSK 250 0
```

Sample 2:

```
12:48:44 x.x.180.116 [11]USER anonymous 331 0
12:48:44 x.x.180.116 [11]PASS IEUser@ 530 1326
12:48:44 x.x.180.116 [12]USER administrator 331 0
12:48:44 x.x.180.116 [12]PASS - 530 1326
```

Sample 3:

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2006-09-23 17:49:32
#Fields: time c-ip cs-username s-sitename s-computername s-ip s-port cs-method cs-uri-stem cs-uri-que
17:57:59 192.168.3.64 Administrator MSFTPSVC1 HAIJO2 192.168.1.12 21 [144]USER Administrator - 331 0
17:57:59 192.168.3.64 Administrator MSFTPSVC1 HAIJO2 192.168.1.12 21 [144]PASS - - 230 0 0 0 16 FTP -
17:58:11 192.168.3.64 Administrator MSFTPSVC1 HAIJO2 192.168.1.12 21 [144]sent /wwwroot/winkel/weekra
17:58:11 192.168.3.64 Administrator MSFTPSVC1 HAIJO2 192.168.1.12 21 [144]sent /wwwroot/winkel/weekra
17:58:11 192.168.3.64 Administrator MSFTPSVC1 HAIJO2 192.168.1.12 21 [144]sent /wwwroot/winkel/weekra
17:58:32 192.168.3.64 Administrator MSFTPSVC1 HAIJO2 192.168.1.12 21 [144]created weekrapport.asp - 2
17:58:42 192.168.3.64 Administrator MSFTPSVC1 HAIJO2 192.168.1.12 21 [144]sent /wwwroot/develop/weekr
17:58:42 192.168.3.64 Administrator MSFTPSVC1 HAIJO2 192.168.1.12 21 [144]sent /wwwroot/develop/weekr
17:58:42 192.168.3.64 Administrator MSFTPSVC1 HAIJO2 192.168.1.12 21 [144]sent /wwwroot/develop/weekr
17:58:49 192.168.3.64 Administrator MSFTPSVC1 HAIJO2 192.168.1.12 21 [144]created weekrapport.asp - 2
17:58:57 192.168.3.64 Administrator MSFTPSVC1 HAIJO2 192.168.1.12 21 [144]QUIT - - 250 0 0 0 0 FTP -
```

Sample 4:

```
2004-12-30 11:24:41 203.115.228.178 ftp MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [12]USER ftp - 331 0 FT

2004-12-30 11:24:41 203.115.228.178 - MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [12]PASS ftp@ftp.net - 53

2004-12-30 11:24:43 203.115.228.178 anyone MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [13]USER anyone - 33

2004-12-30 11:24:43 203.115.228.178 - MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [13]PASS - - 530 1326 FTP

2004-12-30 11:24:44 203.115.228.178 root MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [14]USER root - 331 0

2004-12-30 11:24:44 203.115.228.178 admin MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [15]USER admin - 331

2004-12-30 11:24:44 203.115.228.178 - MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [14]PASS - - 530 1326 FTP

2004-12-30 11:24:44 203.115.228.178 webmaster MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [16]USER webmaste
```

```
2004-12-30 11:24:44 203.115.228.178 - MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [15]PASS - - 530 1326 FTP

2004-12-30 11:24:44 203.115.228.178 user MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [17]USER user - 331 0

2004-12-30 11:24:44 203.115.228.178 - MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [16]PASS - - 530 1326 FTP

2004-12-30 11:24:44 203.115.228.178 test MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [18]USER test - 331 0

2004-12-30 11:24:44 203.115.228.178 - MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [17]PASS - - 530 1326 FTP

2004-12-30 11:24:45 203.115.228.178 web MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [19]USER web - 331 0 FT

2004-12-30 11:24:45 203.115.228.178 - MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [18]PASS - - 530 1326 FTP

2004-12-30 11:24:45 203.115.228.178 www MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [20]USER www - 331 0 FT

2004-12-30 11:24:45 203.115.228.178 - MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [19]PASS - - 530 1326 FTP

2004-12-30 11:24:45 203.115.228.178 administrator MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [22]USER admi

2004-12-30 11:24:45 203.115.228.178 - MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [21]PASS - - 530 1326 FTP

2004-12-30 11:24:45 203.115.228.178 sybase MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [25]USER sybase - 3

2004-12-30 11:24:45 203.115.228.178 - MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [23]PASS - - 530 1326 FTP

2004-12-30 11:24:45 203.115.228.178 - MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [24]PASS - - 530 1326 FTP

2004-12-30 11:24:45 203.115.228.178 user MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [27]USER user - 331 0

2004-12-30 11:24:45 203.115.228.178 webmaster MSFTPSVC1 MULTIMEDIA 192.168.0.203 21 [26]USER webmaste
```

Sample 5:

```
13:15:45 172.28.129.116 [51]USER xxxxx 331 0
13:15:46 172.28.129.116 [51]PASS - 230 0
13:15:56 172.28.129.116 [51]MKD 20051103 257 0
13:15:57 172.28.129.116 [51]CWD 20051103 250 0
13:17:19 172.28.129.116 [51]created /filename 226 0
13:18:44 172.28.129.116 [51]QUIT - 226 0
13:39:13 160.164.22.7 [52]USER anonymous 331 0
13:39:13 160.164.22.7 [52]PASS opss 530 1326
13:39:13 160.164.22.7 [52]QUIT - 530 0
```

Log Samples from ProFTPD

Startup message: ..code-block:: console

May 21 20:20:44 slacker proftpd[25526] proftpd.lab.ossec.net: ProFTPD 1.2.10 (stable) (built Tue Aug 2 22:33:07 PDT 2005) standalone mode STARTUP

Connection attempt: ..code-block:: console

May 21 20:21:18 slacker proftpd[25530] proftpd.lab.ossec.net (192.168.20.10[192.168.20.10]): FTP session opened.

Connection closed: ..code-block:: console

May 21 20:22:14 slacker proftpd[25530] proftpd.lab.ossec.net (192.168.20.10[192.168.20.10]): FTP session closed.

Login sucessful: ..code-block:: console

May 21 20:22:28 slacker proftpd[25556] proftpd.lab.ossec.net (192.168.20.10[192.168.20.10]): USER dcid-test: Login successful.

Login failed: ..code-block:: console

May 21 20:22:44 slacker proftpd[25557] proftpd.lab.ossec.net (192.168.20.10[192.168.20.10]): USER dcid-test (Login failed): Incorrect password.

Invalid user login attempt: ..code-block:: console

May 21 20:21:21 slacker proftpd[25530] proftpd.lab.ossec.net (192.168.20.10[192.168.20.10]): no such user 'dcid-inv'

May 21 20:21:21 slacker proftpd[31806] proftpd.lab.ossec.net (190.48.150.156[190.48.150.156]): USER abad: no such user found from 190.48.150.156 [190.48.150.156] to proftpd.lab.ossec.net:21

Full samples:

```
Jul 14 04:44:46 opala proftpd[30812] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): mod_de
Jul 14 04:44:46 opala proftpd[30813] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): no suc
Jul 14 04:44:46 opala proftpd[30813] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): USER g
Jul 14 04:44:46 opala proftpd[30813] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): mod_de
Jul 14 04:44:46 opala proftpd[30815] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): FTP se
Jul 14 04:44:46 opala proftpd[30814] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): no suc
Jul 14 04:44:46 opala proftpd[30814] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): USER g
Jul 14 04:44:46 opala proftpd[30813] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): FTP se
Jul 14 04:44:46 opala proftpd[30812] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): FTP se
Jul 14 04:44:46 opala proftpd[30815] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): mod_de
Jul 14 04:44:46 opala proftpd[30814] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): FTP se
Jul 14 04:44:47 opala proftpd[30816] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): FTP se
Jul 14 04:44:47 opala proftpd[30817] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): FTP se
Jul 14 04:44:47 opala proftpd[30818] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): FTP se
Jul 14 04:44:47 opala proftpd[30815] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): no suc
Jul 14 04:44:47 opala proftpd[30815] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): USER g
Jul 14 04:44:47 opala proftpd[30816] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): mod_de
Jul 14 04:44:47 opala proftpd[30817] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): mod_de
Jul 14 04:44:47 opala proftpd[30818] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): mod_de
Jul 14 04:44:47 opala proftpd[30815] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): FTP se
Jul 14 04:44:47 opala proftpd[30819] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): FTP se
Jul 14 04:44:47 opala proftpd[30816] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): no suc
Jul 14 04:44:47 opala proftpd[30816] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): USER g
Jul 14 04:44:47 opala proftpd[30816] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): mod_de
Jul 14 04:44:47 opala proftpd[30817] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): no suc
Jul 14 04:44:47 opala proftpd[30817] opala.xxxxxx.edu.br (sieapp.ufpel.edu.br[200.17.161.73]): USER g
```

Log Samples from Pure-FTPD

Connection attempt:

```
pure-ftpd-wrapper[926]: connect from  192.168.20.10 (192.168.20.10)
pure-ftpd: (?@192.168.20.10) [INFO] New connection from 192.168.20.10
```

Connection closed:

```
pure-ftpd: (abcde@192.168.20.10) [INFO] Logout.
```

Login failed:

```
pure-ftpd: (?@192.168.20.10) [WARNING] Authentication failed for user [inv-user]
```

Full Sample:

```
pure-ftpd: (?@24.79.92.194) [WARNING] Authentication failed for user [Administrator]
pure-ftpd: (?@24.79.92.194) [WARNING] Authentication failed for user [Administrator]
pure-ftpd: (?@24.79.92.194) [WARNING] Authentication failed for user [Administrator]
pure-ftpd: (?@24.79.92.194) [WARNING] Authentication failed for user [Administrator]
pure-ftpd: (?@24.79.92.194) [WARNING] Authentication failed for user [Administrator]
pure-ftpd: (?@24.79.92.194) [WARNING] Authentication failed for user [Administrator]
pure-ftpd: (?@24.79.92.194) [WARNING] Authentication failed for user [Administrator]
```

Log Samples from Solaris/HP-UX FTPD

Connection attempt: ..code-block:: console

May 28 15:50:36 sol1 ftpd[28370]: connection from slacker.lab.ossec.net at Sun May 28 15:50:36 2006
May 28 15:50:36 sol1 ftpd[28370]: FTP LOGIN FROM slacker.lab.ossec.net, test-user

Connection refused: ..code-block:: console

Jun 3 13:37:10 sol2 ftpd[327802]: refused connect from spongebob.lab.ossec.net

Login failed: ..code-block:: console

Jun 2 16:44:05 sol2 ftpd[28662]: repeated login failures from spongebob.lab.ossec.net Sep 11 08:59:41 xxx ftpd[18658]: PAM_ERROR_MSG: Account is disabled - see Account Administrator.

Login failed: ..code-block:: console

Jun 2 16:44:05 sol2 ftpd[28662]: repeated login failures from spongebob.lab.ossec.net

Transactions: ..code-block:: console

May 28 19:38:24 sol1 ftpd[24474]: FTPD: IMPORT file local /home/test/file2.tgz, remote Jun 1 22:50:26 sol2 ftpd[22898]: FTPD: IMPORT file local file1.tgz, remote May 28 15:14:02 sol2 ftpd[28616]: FTPD: EXPORT file local , remote aka.html

Mac OS X Server 10.5 FTP logs:

```
Jun 20 09:00:42 File-Server ftpd[65613]: Failed authentication from: [U2FsdGVkX18af1PrJ6KSUhskC8ikcc
Jun 20 09:00:52 File-Server ftpd[65625]: Failed authentication from: [U2FsdGVkX1+RbLXPa7lV2Ly9a3Bir9
Jun 20 09:01:02 File-Server ftpd[65639]: Failed authentication from:  [U2FsdGVkX18V16WdD4Z7rcx6tv0zB
Jun 25 10:24:06 File-Server ftpd[29807]: Failed authentication from: 1.Red-88-2-137.staticIP.rima-td
Jun 25 10:24:25 File-Server ftpd[29871]: Failed authentication from:   1.Red-88-2-137.staticIP.rima-
Jul  4 02:11:44 File-Server ftpd[54844]: FTP LOGIN REFUSED (PASS  before USER) FROM 202.113.244.42 [
```

Log Samples from vsftpd

If the system is using pam, authentication events from vsftp may also be logged in the [[pam|pam format]].
The following are from the vsftpd.log file.

Connection attempt:

```
Mon Jul 10 15:51:17 2006 [pid 26152] CONNECT: Client "192.168.2.10"
```

Failed login:

```
Mon Aug 21 14:33:24 2006 [pid 20175] [dcid] FAIL LOGIN: Client "127.0.0.1"
```

Login OK:

```
Mon Aug 21 14:37:23 2006 [pid 20293] [dcid] OK LOGIN: Client "127.0.0.1"
```

Anonymous login:

```
Mon Aug 21 14:32:06 2006 [pid 20127] [ftp] OK LOGIN: Client "127.0.0.1", anon password "lala@"
```

File upload:

```
Sun Aug 27 16:28:20 2006 [pid 13962] [xx] OK UPLOAD: Client "1.2.3.4", "/a.php", 8338 bytes, 18.77Kby
```

Log Samples from xferlog (by default at /var/log/xferlog)

The xferlog file contains logging information from the FTP server daemon, ftpd. This file usually is found at `/var/log/xferlog`, but can be anywhere else.

Each server entry is composed of a single line of the following form, with all fields being separated by spaces.

```
current-time   transfer-time   remote-host    file-size   filename    transfer-type   special-action-
```

Samples:

```
Thu Sep  2 09:52:00 2004 50 192.168.20.10 896242 /home/test/file1.tgz b _ o r suporte ftp 0 * c
Thu Sep  2 09:57:16 2004 289 192.168.20.10 8045867 /home/test2.tgz b _ o r suporte ftp 0 * c
```

Nessus scan in a web server log

How ossec would alert

Misc. Logs

Amavis Logs

Log entries for Amavis from /var/log/maillog:

Log Samples from Aruba Wireless

Log Samples from Asterisk

```
Dec 16 18:02:04 asterisk1 asterisk[31774]: NOTICE[31787]: chan_sip.c:11242 in handle_request_register
Dec 16 18:03:13 asterisk1 asterisk[31774]: NOTICE[31787]: chan_sip.c:11242 in handle_request_register
Dec 16 18:04:49 asterisk1 asterisk[31774]: NOTICE[31787]: chan_sip.c:11242 in handle_request_register
Dec 16 18:04:49 asterisk1 asterisk[31774]: NOTICE[31787]: chan_sip.c:11242 in handle_request_register
Jun 27 18:09:47 host asterisk[31774]: ERROR[27910]: chan_zap.c:10314 setup_zap: Unable to register ch
Jun 27 18:09:47 host asterisk[31774]: WARNING[27910]: loader.c:414 __load_resource: chan_zap.so: load
Jun 27 18:09:47 host asterisk[31774]: WARNING[27910]: loader.c:554 load_modules: Loading module chan_
```

Log samples from ClamAV

```
Jul  9 09:04:05 s69819 clamd[11292]: stream: HTML.Phishing.Pay-33 FOUND
Jul  9 11:40:02 s69819 clamd[11292]: stream: HTML.Phishing.Auction-111 FOUND
Jul  9 16:41:40 s69819 clamd[11292]: stream: HTML.Phishing.Pay-33 FOUND
Jul  9 16:45:26 s69819 clamd[11292]: stream: HTML.Phishing.Pay-33 FOUND
Jul  9 18:35:27 s69819 clamd[11292]: stream: HTML.Phishing.Pay-110 FOUND
Jul  9 21:00:06 s69819 clamd[11292]: stream: HTML.Phishing.Auction-111 FOUND
Jul 10 01:48:16 s69819 clamd[11292]: stream: HTML.Phishing.Pay-33 FOUND
Jul 10 03:35:54 s69819 clamd[11292]: stream: HTML.Phishing.Pay-110 FOUND
Jul 10 04:40:36 s69819 clamd[11292]: stream: HTML.Phishing.Auction-111 FOUND
Jul 10 06:29:49 s69819 clamd[11292]: stream: HTML.Phishing.Acc-4 FOUND
Jul 10 06:30:06 s69819 clamd[11292]: stream: HTML.Phishing.Acc-4 FOUND
Jul 10 16:57:19 s69819 clamd[11292]: stream: HTML.Phishing.Pay-110 FOUND
Jul 11 00:04:58 s69819 clamd[11292]: stream: HTML.Phishing.Pay-110 FOUND
Jul 11 09:00:06 s69819 clamd[11292]: stream: HTML.Phishing.Pay-110 FOUND
Jul 11 13:03:46 s69819 clamd[11292]: stream: HTML.Phishing.Auction-111 FOUND
Jul 11 19:51:21 s69819 clamd[11292]: stream: HTML.Phishing.Pay-110 FOUND
Jul 12 06:04:38 s69819 clamd[11292]: stream: HTML.Phishing.Pay-130 FOUND
Jul 12 13:41:55 s69819 clamd[11292]: stream: Worm.SomeFool.P FOUND
Jul 12 21:20:03 s69819 clamd[11292]: stream: HTML.Phishing.Pay-147 FOUND
Jul  2 06:34:56 s69819 clamd[20016]: stream: HTML.Phishing.Acc-4 FOUND
Jul  2 14:31:45 s69819 clamd[20016]: stream: HTML.Phishing.Acc-4 FOUND
Jul  2 17:50:54 s69819 clamd[11292]: stream: HTML.Phishing.Bank-497 FOUND
Jul  3 19:00:44 s69819 clamd[11292]: stream: HTML.Phishing.Auction-93 FOUND
Jul  4 02:57:06 s69819 clamd[11292]: stream: HTML.Phishing.Pay-51 FOUND
Jul  4 09:32:26 s69819 clamd[11292]: stream: HTML.Phishing.Acc-4 FOUND
Jul  4 11:20:08 s69819 clamd[11292]: stream: HTML.Phishing.Bank-475 FOUND
Jul  4 17:27:51 s69819 clamd[11292]: stream: HTML.Phishing.Pay-6 FOUND
Jul  4 19:01:05 s69819 clamd[11292]: stream: HTML.Phishing.Bank-490 FOUND
Jul  5 12:35:44 s69819 clamd[11292]: stream: Worm.SomeFool.P FOUND
```

```
Jul  5 16:42:24 s69819 clamd[11292]: stream: Exploit.HTML.IFrame FOUND
Jul  5 17:23:46 s69819 clamd[11292]: stream: Worm.SomeFool.Gen-2 FOUND
Jul  5 18:10:58 s69819 clamd[11292]: stream: HTML.Phishing.Pay-51 FOUND
Jul  5 20:27:00 s69819 clamd[11292]: stream: HTML.Phishing.Bank-546 FOUND
Jul  6 02:28:58 s69819 clamd[11292]: stream: HTML.Phishing.Bank-551 FOUND
Jul  6 15:16:18 s69819 clamd[11292]: stream: HTML.Phishing.Pay-37 FOUND
Jul  6 19:08:46 s69819 clamd[11292]: stream: HTML.Phishing.Pay-37 FOUND
Jul  7 05:20:35 s69819 clamd[11292]: stream: HTML.Phishing.Pay-130 FOUND
Jul  7 07:49:16 s69819 clamd[11292]: stream: HTML.Phishing.Pay-37 FOUND
Jul  7 17:25:14 s69819 clamd[11292]: stream: HTML.Phishing.Pay-33 FOUND
Jul  7 18:21:56 s69819 clamd[11292]: stream: HTML.Phishing.Pay-106 FOUND
Jul  8 04:30:32 s69819 clamd[11292]: stream: HTML.Phishing.Auction-102 FOUND
Jul  8 08:51:46 s69819 clamd[11292]: stream: HTML.Phishing.Pay-33 FOUND
Jul  8 10:15:01 s69819 clamd[11292]: stream: HTML.Phishing.Pay-152 FOUND
Jul  8 16:24:46 s69819 clamd[11292]: stream: HTML.Phishing.Pay-33 FOUND
```

Log Samples for Dell OpenManage

```
Sep  2 15:33:53 gateway1 Server Administrator: Instrumentation Service EventID: 1354  Power supply de
Sep  2 15:33:53 gateway1 Server Administrator: Instrumentation Service EventID: 1012  IPMI status  In
Sep  2 15:33:53 gateway1 Server Administrator: Instrumentation Service EventID: 1001  Server Administ
Sep  2 15:33:53 gateway1 Server Administrator: Storage Service EventID: 2164  See readme.txt for a li
Sep  2 15:44:54 gateway1 Server Administrator: Instrumentation Service EventID: 1000  Server Administ
Sep  2 15:44:54 gateway1 Server Administrator: Instrumentation Service EventID: 1306  Redundancy lost
Sep  2 15:44:54 gateway1 Server Administrator: Instrumentation Service EventID: 1354  Power supply de
Sep  2 15:44:54 gateway1 Server Administrator: Instrumentation Service EventID: 1012  IPMI status  In
Sep  2 15:44:54 gateway1 Server Administrator: Instrumentation Service EventID: 1001  Server Administ
Sep  2 15:44:55 gateway1 Server Administrator: Storage Service EventID: 2164  See readme.txt for a li
Sep  4 19:20:00 gateway1 Server Administrator: Instrumentation Service EventID: 1000  Server Administ
Sep  4 19:20:00 gateway1 Server Administrator: Instrumentation Service EventID: 1306  Redundancy lost
Sep  4 19:20:00 gateway1 Server Administrator: Instrumentation Service EventID: 1354  Power supply de
Sep  4 19:20:00 gateway1 Server Administrator: Instrumentation Service EventID: 1012  IPMI status  In
Sep  4 19:20:00 gateway1 Server Administrator: Instrumentation Service EventID: 1001  Server Administ
Sep  4 19:20:00 gateway1 Server Administrator: Storage Service EventID: 2164  See readme.txt for a li
Sep  4 21:20:24 gateway1 Server Administrator: Instrumentation Service EventID: 1053  Temperature ser
Sep  4 21:21:16 gateway1 Server Administrator: Instrumentation Service EventID: 1052  Temperature ser
```

Log samples for HP-UX cimserver

```
Dec 18 18:06:28 hostname cimserver[18575]: PGS17200: Authentication failed for user jones_b.
Dec 18 18:06:29 hostname cimserver[18575]: PGS17200: Authentication failed for user domain\jones_b.
```

Stunnel Logs

Here is a log sample from Stunnel for Windows

Filename = C:Program FilesStunnelstunnel.log

```
2006.11.18 23:28:27 LOG5[900:924]: stunnel 4.16 on x86-pc-mingw32-gnu with OpenSSL 0.9.7i 14 Oct 2005
2006.11.18 23:28:27 LOG5[900:924]: Threading:WIN32 SSL:ENGINE Sockets:SELECT,IPv6
2006.11.18 23:28:36 LOG5[900:208]: No limit detected for the number of clients
2006.11.19 07:11:32 LOG5[856:864]: stunnel 4.16 on x86-pc-mingw32-gnu with OpenSSL 0.9.7i 14 Oct 2005
2006.11.19 07:11:32 LOG5[856:864]: Threading:WIN32 SSL:ENGINE Sockets:SELECT,IPv6
```

```
2006.11.19 07:11:41 LOG5[856:208]: No limit detected for the number of clients
2006.11.19 12:03:45 LOG5[856:1916]: TightVNC connected from 10.54.27.8:3891
2006.11.19 12:03:45 LOG5[856:1916]: Connection closed: 299 bytes sent to SSL, 400 bytes sent to socke
2006.11.19 12:03:52 LOG5[856:1372]: TightVNC connected from 10.54.27.8:3893
2006.11.19 12:03:52 LOG5[856:1372]: Connection closed: 168 bytes sent to SSL, 331 bytes sent to socke
2006.11.19 12:03:53 LOG5[856:2000]: TightVNC connected from 10.54.27.8:3895
2006.11.19 12:03:54 LOG5[856:2000]: Connection closed: 49607 bytes sent to SSL, 316 bytes sent to soc
2006.11.19 12:03:55 LOG5[856:1412]: TightVNC connected from 10.54.27.8:3897
2006.11.19 12:03:55 LOG5[856:1412]: Connection closed: 49607 bytes sent to SSL, 244 bytes sent to soc
2006.11.19 12:03:55 LOG5[856:1140]: TightVNC connected from 10.54.27.8:3899
2006.11.19 12:03:55 LOG5[856:1140]: Connection closed: 49607 bytes sent to SSL, 316 bytes sent to soc
2006.11.19 12:04:05 LOG5[856:1400]: TightVNC2 connected from 10.54.27.8:3901
2006.11.19 12:04:05 LOG5[856:1400]: Connection closed: 36 bytes sent to SSL, 28 bytes sent to socket
2006.11.19 12:04:08 LOG5[856:1416]: TightVNC2 connected from 10.54.27.8:3903
2006.11.19 12:15:41 LOG5[856:1416]: Connection closed: 3237463 bytes sent to SSL, 35933 bytes sent to
2006.11.19 12:15:44 LOG5[856:1752]: TightVNC connected from 10.54.27.8:3921
2006.11.19 12:15:44 LOG5[856:1752]: Connection closed: 299 bytes sent to SSL, 433 bytes sent to socke
2006.11.19 12:15:52 LOG5[856:3856]: TightVNC2 connected from 10.54.27.8:3923
2006.11.19 12:30:45 LOG5[856:3856]: Connection closed: 1414271 bytes sent to SSL, 10775 bytes sent to
2006.11.19 20:15:35 LOG5[856:1952]: TightVNC connected from 10.54.27.8:2421
2006.11.19 20:15:35 LOG5[856:1952]: Connection closed: 299 bytes sent to SSL, 400 bytes sent to socke
2006.11.19 20:15:43 LOG5[856:3032]: TightVNC connected from 10.54.27.8:2423
2006.11.19 20:15:43 LOG5[856:3032]: Connection closed: 168 bytes sent to SSL, 331 bytes sent to socke
2006.11.19 20:15:44 LOG5[856:3172]: TightVNC connected from 10.54.27.8:2425
2006.11.19 20:15:44 LOG5[856:3172]: Connection closed: 49607 bytes sent to SSL, 316 bytes sent to soc
2006.11.19 20:15:45 LOG5[856:3672]: TightVNC connected from 10.54.27.8:2427
2006.11.19 20:15:45 LOG5[856:3672]: Connection closed: 49607 bytes sent to SSL, 244 bytes sent to soc
2006.11.19 20:15:45 LOG5[856:3696]: TightVNC connected from 10.54.27.8:2429
2006.11.19 20:15:45 LOG5[856:3696]: Connection closed: 49607 bytes sent to SSL, 316 bytes sent to soc
2006.11.19 20:15:51 LOG5[856:3800]: TightVNC2 connected from 10.54.27.8:2431
```

Log entries made while a portscan was taking place:

```
2006.11.19 20:36:44 LOG5[856:1540]: TightVNC connected from 10.54.27.5:42557
2006.11.19 20:36:44 LOG3[856:1540]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:36:44 LOG5[856:1540]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:36:49 LOG5[856:2344]: TightVNC connected from 10.54.27.5:42570
2006.11.19 20:36:49 LOG3[856:2344]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:36:49 LOG5[856:2344]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:36:54 LOG5[856:3504]: TightVNC connected from 10.54.27.5:42571
2006.11.19 20:36:54 LOG3[856:3504]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:36:54 LOG5[856:3504]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:36:59 LOG5[856:3208]: TightVNC connected from 10.54.27.5:42572
2006.11.19 20:36:59 LOG3[856:3208]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:36:59 LOG5[856:3208]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:37:04 LOG5[856:2944]: TightVNC connected from 10.54.27.5:42573
2006.11.19 20:37:04 LOG3[856:2944]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:37:04 LOG5[856:2944]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:37:09 LOG5[856:2428]: TightVNC connected from 10.54.27.5:42574
2006.11.19 20:37:09 LOG3[856:2428]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:37:09 LOG5[856:2428]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:37:14 LOG5[856:2044]: TightVNC connected from 10.54.27.5:42575
2006.11.19 20:37:14 LOG3[856:2044]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:37:14 LOG5[856:2044]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:37:19 LOG5[856:1648]: TightVNC connected from 10.54.27.5:42576
2006.11.19 20:37:19 LOG3[856:1648]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:37:19 LOG5[856:1648]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:37:24 LOG5[856:2436]: TightVNC connected from 10.54.27.5:42577
```

```
2006.11.19 20:37:24 LOG3[856:2436]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:37:24 LOG5[856:2436]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:37:29 LOG5[856:3284]: TightVNC connected from 10.54.27.5:42578
2006.11.19 20:37:29 LOG3[856:3284]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:37:29 LOG5[856:3284]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:37:34 LOG5[856:3356]: TightVNC connected from 10.54.27.5:42579
2006.11.19 20:37:34 LOG3[856:3356]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:37:34 LOG5[856:3356]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:37:39 LOG5[856:3404]: TightVNC connected from 10.54.27.5:42580
2006.11.19 20:37:39 LOG3[856:3404]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:37:39 LOG5[856:3404]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:37:44 LOG5[856:2928]: TightVNC connected from 10.54.27.5:42581
2006.11.19 20:37:44 LOG3[856:2928]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:37:44 LOG5[856:2928]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:37:49 LOG5[856:1380]: TightVNC connected from 10.54.27.5:42582
2006.11.19 20:37:49 LOG3[856:1380]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:37:49 LOG5[856:1380]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:37:54 LOG5[856:2068]: TightVNC connected from 10.54.27.5:42583
2006.11.19 20:37:54 LOG3[856:2068]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:37:54 LOG5[856:2068]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:37:59 LOG5[856:3896]: TightVNC connected from 10.54.27.5:42584
2006.11.19 20:37:59 LOG3[856:3896]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:37:59 LOG5[856:3896]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:04 LOG5[856:3252]: TightVNC connected from 10.54.27.5:42585
2006.11.19 20:38:04 LOG3[856:3252]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:38:04 LOG5[856:3252]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:09 LOG5[856:3168]: TightVNC connected from 10.54.27.5:42586
2006.11.19 20:38:09 LOG3[856:3168]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:38:09 LOG5[856:3168]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:11 LOG5[856:3280]: imaps connected from 10.54.27.5:42557
2006.11.19 20:38:11 LOG3[856:3280]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:38:11 LOG5[856:3280]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:16 LOG5[856:3804]: TightVNC connected from 10.54.27.5:42587
2006.11.19 20:38:16 LOG3[856:3804]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:38:16 LOG5[856:3804]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:19 LOG5[856:2816]: ssmtp connected from 10.54.27.5:42557
2006.11.19 20:38:19 LOG3[856:2816]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:38:19 LOG5[856:2816]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:24 LOG5[856:1736]: TightVNC connected from 10.54.27.5:42588
2006.11.19 20:38:24 LOG3[856:1736]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:38:24 LOG5[856:1736]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:27 LOG5[856:1544]: TightVNC2 connected from 10.54.27.5:42557
2006.11.19 20:38:27 LOG3[856:1544]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:38:27 LOG5[856:1544]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:32 LOG5[856:3220]: TightVNC connected from 10.54.27.5:42589
2006.11.19 20:38:32 LOG3[856:3220]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:38:32 LOG5[856:3220]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:37 LOG5[856:2804]: TightVNC connected from 10.54.27.5:42590
2006.11.19 20:38:37 LOG3[856:2804]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:38:37 LOG5[856:2804]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:42 LOG5[856:3196]: TightVNC connected from 10.54.27.5:42591
2006.11.19 20:38:42 LOG3[856:3196]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:38:42 LOG5[856:3196]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:47 LOG5[856:3772]: TightVNC connected from 10.54.27.5:42592
2006.11.19 20:38:47 LOG3[856:3772]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:38:47 LOG5[856:3772]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:52 LOG5[856:3820]: TightVNC connected from 10.54.27.5:42593
2006.11.19 20:38:52 LOG3[856:3820]: SSL_accept: Peer suddenly disconnected
```

```
2006.11.19 20:38:52 LOG5[856:3820]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:38:57 LOG5[856:3152]: TightVNC connected from 10.54.27.5:42594
2006.11.19 20:38:57 LOG3[856:3152]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:38:57 LOG5[856:3152]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:39:02 LOG5[856:2408]: TightVNC connected from 10.54.27.5:42595
2006.11.19 20:39:02 LOG3[856:2408]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:39:02 LOG5[856:2408]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:39:07 LOG5[856:2056]: TightVNC connected from 10.54.27.5:42596
2006.11.19 20:39:07 LOG3[856:2056]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:39:07 LOG5[856:2056]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 20:40:08 LOG5[856:2856]: pop3s connected from 10.54.27.5:42557
2006.11.19 20:40:08 LOG3[856:2856]: SSL_accept: Peer suddenly disconnected
2006.11.19 20:40:08 LOG5[856:2856]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
```

More log samples:

```
2006.11.19 21:01:29 LOG5[856:3800]: Connection closed: 5567666 bytes sent to SSL, 122583 bytes sent t
2006.11.19 22:55:50 LOG5[856:4052]: TightVNC2 connected from 10.54.27.8:4443
2006.11.19 22:55:50 LOG3[856:4052]: SSL_read: Connection reset by peer (WSAECONNRESET) (10054)
2006.11.19 22:55:50 LOG5[856:4052]: Connection reset: 12 bytes sent to SSL, 0 bytes sent to socket
2006.11.19 22:56:31 LOG5[856:1824]: TightVNC connected from 10.54.27.8:4444
2006.11.19 22:56:31 LOG3[856:1824]: SSL_read: Connection reset by peer (WSAECONNRESET) (10054)
2006.11.19 22:56:31 LOG5[856:1824]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.20 00:25:31 LOG5[856:3104]: TightVNC connected from 10.54.27.8:4533
2006.11.20 00:25:31 LOG3[856:3104]: SSL_read: Connection reset by peer (WSAECONNRESET) (10054)
2006.11.20 00:25:31 LOG5[856:3104]: Connection reset: 0 bytes sent to SSL, 0 bytes sent to socket
2006.11.20 00:25:41 LOG5[856:2848]: TightVNC2 connected from 10.54.27.8:4535
2006.11.20 00:25:41 LOG3[856:2848]: SSL_read: Connection reset by peer (WSAECONNRESET) (10054)
2006.11.20 00:25:41 LOG5[856:2848]: Connection reset: 12 bytes sent to SSL, 0 bytes sent to socket
2006.11.20 00:48:57 LOG5[856:3964]: TightVNC connected from 10.54.27.8:1072
2006.11.20 00:48:57 LOG5[856:3964]: Connection closed: 299 bytes sent to SSL, 400 bytes sent to socke
2006.11.20 00:49:04 LOG5[856:3712]: TightVNC2 connected from 10.54.27.8:1074
2006.11.20 00:55:34 LOG5[856:3712]: Connection closed: 3405756 bytes sent to SSL, 43743 bytes sent to
```

TightVNC Logs

Here is a log sample from TightVNC for Windows (Server version 1.2.9)

Filename = C:WindowsSystem32WinVNC.log

```
vncServer.cpp : trying port number 5900
Sun Nov 19 07:11:42 2006
vncSockConnect.cpp : started socket connection thread
Sun Nov 19 12:03:45 2006
vncHTTPConnect.cpp : HTTP client connected
vncHTTPConnect.cpp : file / requested
vncHTTPConnect.cpp : sending main page
vncService.cpp : SelectHDESK failed to close old desktop 28, error=170
Sun Nov 19 12:03:52 2006
vncHTTPConnect.cpp : HTTP client connected
vncHTTPConnect.cpp : file /favicon.ico requested
Sun Nov 19 12:03:53 2006
vncHTTPConnect.cpp : HTTP client connected
vncHTTPConnect.cpp : file /VncViewer.jar requested
Sun Nov 19 12:03:55 2006
vncHTTPConnect.cpp : HTTP client connected
```

```
vncHTTPConnect.cpp : file /VncViewer.jar requested
vncHTTPConnect.cpp : HTTP client connected
vncHTTPConnect.cpp : file /VncViewer.jar requested
Sun Nov 19 12:04:05 2006
vncSockConnect.cpp : accepted connection from 127.0.0.1
vncClient.cpp : client connected : 127.0.0.1 (id 1)
vncClient.cpp : authentication failed
Sun Nov 19 12:04:08 2006
vncSockConnect.cpp : accepted connection from 127.0.0.1
vncClient.cpp : client connected : 127.0.0.1 (id 1)
Sun Nov 19 12:04:10 2006
vncService.cpp : SelectHDESK failed to close old desktop 28, error=170
vncService.cpp : SelectHDESK failed to close old desktop 28, error=170
vncMenu.cpp : KillActiveDesktop
Sun Nov 19 12:04:25 2006
vncDesktop.cpp : display resolution or desktop changed.
Sun Nov 19 12:15:41 2006
vncClient.cpp : client disconnected : 127.0.0.1 (id 1)
vncServer.cpp : deleting desktop server
Sun Nov 19 12:15:44 2006
vncHTTPConnect.cpp : HTTP client connected
vncHTTPConnect.cpp : file / requested
vncHTTPConnect.cpp : sending main page
vncService.cpp : SelectHDESK failed to close old desktop 28, error=170
Sun Nov 19 12:15:52 2006
vncSockConnect.cpp : accepted connection from 127.0.0.1
vncClient.cpp : client connected : 127.0.0.1 (id 1)
vncMenu.cpp : KillActiveDesktop
Sun Nov 19 12:30:45 2006
vncService.cpp : SelectHDESK failed to close old desktop 28, error=170
vncClient.cpp : client disconnected : 127.0.0.1 (id 1)
vncServer.cpp : deleting desktop server
vncService.cpp : SelectHDESK failed to close old desktop 28, error=170
Sun Nov 19 20:15:35 2006
vncHTTPConnect.cpp : HTTP client connected
vncHTTPConnect.cpp : file / requested
vncHTTPConnect.cpp : sending main page
vncService.cpp : SelectHDESK failed to close old desktop 28, error=170
Sun Nov 19 20:15:43 2006
vncHTTPConnect.cpp : HTTP client connected
vncHTTPConnect.cpp : file /favicon.ico requested
Sun Nov 19 20:15:44 2006
vncHTTPConnect.cpp : HTTP client connected
vncHTTPConnect.cpp : file /VncViewer.jar requested
Sun Nov 19 20:15:45 2006
vncHTTPConnect.cpp : HTTP client connected
vncHTTPConnect.cpp : file /VncViewer.jar requested
vncHTTPConnect.cpp : HTTP client connected
vncHTTPConnect.cpp : file /VncViewer.jar requested
Sun Nov 19 20:15:51 2006
vncSockConnect.cpp : accepted connection from 127.0.0.1
vncClient.cpp : client connected : 127.0.0.1 (id 1)
vncService.cpp : SelectHDESK failed to close old desktop 28, error=170
vncService.cpp : SelectHDESK failed to close old desktop 28, error=170
vncMenu.cpp : KillActiveDesktop
Sun Nov 19 20:15:55 2006
vncDesktop.cpp : display resolution or desktop changed.
Sun Nov 19 20:57:29 2006
```

```
vncDesktop.cpp : display resolution or desktop changed.
Sun Nov 19 21:00:59 2006
vncDesktop.cpp : display resolution or desktop changed.
Sun Nov 19 21:01:29 2006
vncClient.cpp : client disconnected : 127.0.0.1 (id 1)
vncServer.cpp : deleting desktop server
Sun Nov 19 22:55:50 2006
vncSockConnect.cpp : accepted connection from 127.0.0.1
vncClient.cpp : client connected : 127.0.0.1 (id 1)
Sun Nov 19 22:56:31 2006
vncHTTPConnect.cpp : HTTP client connected
Mon Nov 20 00:25:31 2006
vncHTTPConnect.cpp : HTTP client connected
Mon Nov 20 00:25:41 2006
vncSockConnect.cpp : accepted connection from 127.0.0.1
vncClient.cpp : client connected : 127.0.0.1 (id 1)
Mon Nov 20 00:48:57 2006
vncHTTPConnect.cpp : HTTP client connected
vncHTTPConnect.cpp : file / requested
vncHTTPConnect.cpp : sending main page
vncService.cpp : SelectHDESK failed to close old desktop 28, error=170
Mon Nov 20 00:49:04 2006
vncSockConnect.cpp : accepted connection from 127.0.0.1
vncClient.cpp : client connected : 127.0.0.1 (id 1)
vncService.cpp : SelectHDESK failed to close old desktop 28, error=170
vncService.cpp : SelectHDESK failed to close old desktop 28, error=170
vncMenu.cpp : KillActiveDesktop
Mon Nov 20 00:49:08 2006
vncDesktop.cpp : display resolution or desktop changed.
Mon Nov 20 00:55:34 2006
vncClient.cpp : client disconnected : 127.0.0.1 (id 1)
vncServer.cpp : deleting desktop server
```

Log Samples for Wordpress

```
Aug 11 17:45:34 ourhome WPsyslog[13016]: [127.0.0.1 admin] Info: Module:wpsyslog WPsyslog configurati
Aug 11 17:46:27 ourhome WPsyslog[13019]: [127.0.0.1 admin] Info: Module:wpsyslog WPsyslog configurati
Aug 11 17:54:48 ourhome WPsyslog[13092]: [127.0.0.1 na] Notice: Comment posted. Comment Id: #7, name
Aug 11 18:12:25 ourhome WPsyslog[13016]: [127.0.0.1 admin] Warning: Plugin deactivated. Plugin name:
Aug 11 18:14:57 ourhome WPsyslog[13019]: [127.0.0.1 admin] Warning: Plugin deactivated. Plugin name:
Aug 11 18:24:55 ourhome WPsyslog[13295]: [127.0.0.1 admin] Info: WPsyslog was successfully initialise
Aug 11 18:25:41 ourhome WPsyslog[14382]: [127.0.0.1 na] Info: User logged in. User name: admin (admin
Aug 11 18:25:55 ourhome WPsyslog[14382]: [127.0.0.1 admin] Info: User logged out. User name: admin (a
Aug 11 18:26:05 ourhome WPsyslog[14382]: [127.0.0.1 na] Info: User authentication failed. User name:
Aug 11 18:26:17 ourhome WPsyslog[14382]: [127.0.0.1 na] Info: User authentication failed. User name:
Aug 11 18:48:47 ourhome WPsyslog[13019]: [127.0.0.1 admin] Info: WPsyslog configuration has been char
Aug 11 18:49:48 ourhome WPsyslog[13015]: [127.0.0.1 admin] Warning: Plugin deactivated. Plugin name:
Aug 11 18:52:59 ourhome WPsyslog[13295]: [127.0.0.1 admin] Warning: Plugin deactivated. Plugin name:
Aug 11 18:52:59 ourhome WPsyslog[13295]: [127.0.0.1 admin] Warning: WPsyslog plugin has been deactiva
Aug 11 18:53:03 ourhome WPsyslog[13295]: [127.0.0.1 admin] Warning: WPsyslog plugin has been activate
```

Cisco Logs

Log samples for the Cisco IDS/IPS module for IOS

Sep 1 10:38:36 10.10.10.1 614: *Sep 1 17:36:34.303: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:36 10.10.10.1 615: *Sep 1 17:36:34.307: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:36 10.10.10.1 616: *Sep 1 17:36:34.531: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:36 10.10.10.1 617: *Sep 1 17:36:34.531: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:36 10.10.10.1 618: *Sep 1 17:36:34.783: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:36 10.10.10.1 619: *Sep 1 17:36:34.783: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:36 10.10.10.1 620: *Sep 1 17:36:35.087: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:36 10.10.10.1 621: *Sep 1 17:36:35.087: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:36 10.10.10.1 622: *Sep 1 17:36:35.495: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:37 10.10.10.1 623: *Sep 1 17:36:35.495: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:37 10.10.10.1 624: *Sep 1 17:36:36.111: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:37 10.10.10.1 625: *Sep 1 17:36:36.111: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:39 10.10.10.1 626: *Sep 1 17:36:37.047: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:39 10.10.10.1 627: *Sep 1 17:36:37.047: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:41 10.10.10.1 628: *Sep 1 17:36:38.719: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:41 10.10.10.1 629: *Sep 1 17:36:38.719: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80] Sep 1 10:38:49 10.10.10.1 630: *Sep 1 17:36:46.715: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:52032 -> 10.10.10.10:80] Sep 1 10:38:50 10.10.10.1 631: *Sep 1 17:36:48.199: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:54000 -> 10.10.10.10:80] Sep 1 10:38:58 10.10.10.1 632: *Sep 1 17:36:55.827: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:63596 -> 10.10.10.10:4444] Sep 1 10:38:58 10.10.10.1 633: *Sep 1 17:36:55.827: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:49486 -> 10.10.10.10:80] Sep 1 10:38:58 10.10.10.1 634: *Sep 1 17:36:55.831: %IPS-4-SIGNATURE: Sig:5123 Subsig:2 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:49486 -> 10.10.10.10:80] Sep 1 10:38:59 10.10.10.1 635: *Sep 1 17:36:56.831: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:59499 -> 10.10.10.10:4444] Sep 1 10:38:59 10.10.10.1 636: *Sep 1 17:36:56.883: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:56017 -> 10.10.10.10:4444] Sep 1 10:39:29 10.10.10.1 647: *Sep 1 17:37:28.027: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:60915 -> 10.10.10.10:80] Sep 1 10:39:29 10.10.10.1 648: *Sep 1 17:37:28.031: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:29 10.10.10.1 649: *Sep 1 17:37:28.035: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:29 10.10.10.1 650: *Sep 1 17:37:28.259: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:30 10.10.10.1 651: *Sep 1 17:37:28.511: %IPS-4-SIGNATURE: Sig:5123

Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:30 10.10.10.1 652: *Sep 1 17:37:28.511: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:30 10.10.10.1 653: *Sep 1 17:37:28.815: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:30 10.10.10.1 654: *Sep 1 17:37:28.815: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:30 10.10.10.1 655: *Sep 1 17:37:29.223: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:31 10.10.10.1 656: *Sep 1 17:37:29.223: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:31 10.10.10.1 657: *Sep 1 17:37:29.839: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:31 10.10.10.1 658: *Sep 1 17:37:29.839: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:33 10.10.10.1 659: *Sep 1 17:37:30.775: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:33 10.10.10.1 660: *Sep 1 17:37:30.775: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:34 10.10.10.1 661: *Sep 1 17:37:32.447: %IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:34 10.10.10.1 662: *Sep 1 17:37:32.447: %IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:54068 -> 10.10.10.10:80] Sep 1 10:39:36 10.10.10.1 663: *Sep 1 17:37:34.523: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.12:1246 -> 192.168.100.1:443] Sep 1 10:39:47 10.10.10.1 664: *Sep 1 17:37:45.607: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.12:1247 -> 192.168.100.1:443] Sep 1 10:40:41 10.10.10.1 665: *Sep 1 17:38:39.303: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.12:1248 -> 192.168.100.1:443] Sep 1 10:41:06 10.10.10.1 666: *Sep 1 17:39:03.795: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.12:1249 -> 192.168.100.1:443] Sep 1 10:41:18 10.10.10.1 667: *Sep 1 17:39:15.995: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.12:1250 -> 192.168.100.1:443] Sep 1 10:42:08 10.10.10.1 678: *Sep 1 17:40:06.271: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.12:1251 -> 192.168.100.1:443] Sep 1 10:44:39 10.10.10.1 695: *Sep 1 17:42:37.623: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.12:1252 -> 192.168.100.1:443]

Cisco IOS Samples

Full log sample:

Sep 6 09:13:00 RouterName 82: Sep 6 14:12:56.872: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 09:13:01 RouterName 83: Sep 6 14:12:57.872: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 1.1.1.1 started - CLI initiated Sep 6 09:14:42 RouterName 84: Sep 6 14:14:39.048: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 09:18:13 RouterName 85: Sep 6 14:18:10.047: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 09:20:44 RouterName 86: Sep 6 14:20:35.991: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 09:20:45 RouterName 87: Sep 6 14:20:41.991: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 1.1.1.1 stopped - CLI initiated Sep 6 09:20:45 RouterName 88: Sep 6 14:20:41.991: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 1.1.1.1 started - CLI initiated Sep 6 09:25:12 RouterName 89: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 12:42:16 RouterName 90: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 12:42:47 RouterName 91: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 12:44:52 RouterName 92: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 7 06:20:59 RouterName 93: SSH2 0: Unexpected message received Sep 7 07:02:56 RouterName 94: SSH2 0: Unexpected mesg type received Sep 7 13:18:06 Router-

Name 95: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 7 13:18:06 RouterName 96: %SEC-6-IPACCESSLOGP: list 120 denied udp 10.0.0.66(137) -> 10.0.0.11(137), 33 packets

Access list (full timestamp and message id):

Jul 10 16:07:14 cisco2621 636: .Jul 10 15:58:56.590 EDT: %SEC-6-IPACCESSLOGP: list 102 denied tcp 10.0.6.56(3067) -> 172.36.4.7(139), 1 packet

123: May 3 05:15:25.217 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.0.40.16(3059) -> 10.0.4.101(1060), 2 packets 124: May 3 05:15:27.302 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.0.16.16(2179) -> 10.0.4.101(1060), 1 packet 125: May 3 05:15:40.362 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.0.32.16(4206) -> 10.0.4.101(1060), 2 packets 126: May 3 05:15:42.790 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.131.5.17(3737) -> 10.0.4.101(445), 1 packet

127: May 3 05:23:33.404 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1477) -> 10.0.127.20(445), 1 packet 128: May 3 05:23:34.416 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1469) -> 10.0.127.12(445), 1 packet 129: May 3 05:23:35.524 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1473) -> 10.0.127.16(445), 1 packet 130: May 3 05:23:36.528 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1478) -> 10.0.127.21(445), 1 packet 131: May 3 05:23:37.528 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1496) -> 10.0.127.39(445), 1 packet 132: May 3 05:23:38.540 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1484) -> 10.0.127.27(445), 1 packet

4872: Dec 11 08:02:53.887 pst: %SEC-6-IPACCESSLOGP: list 100 denied udp 200.174.153.126(1028) -> 66.81.85.65(137), 1 packet 4873: Dec 11 08:03:09.583 pst: %SEC-6-IPACCESSLOGP: list 100 denied udp 195.23.72.148(1026) -> 66.81.85.65(137), 1 packet

Configured:

Jun 12 14:22:25 site1 1348: .Jun 12 18:22:22 UTC: %SYS-5-CONFIG_I: Configured from 127.0.0.21 by snmp

Cisco PIX Logs

Log Samples from the Cisco PIX: The Cisco PIX logs are very well formatted and easy to parse. Every message starts with a unique ID of the event, which is in the following format: <b>%PIX-severity-eventID. A complete list with all event IDS can be found at the : [http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guide_chapter09186a008051a0ca.html cisco site]. [http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/syslog/pixemsgs.htm Cisco Pix Specific].

Full log samples:

```
Sep  7 06:25:17 PIXName %PIX-7-710005: UDP request discarded from 0.0.0.0/68 to outside:255.255.255.2
Sep  7 06:25:23 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/13
Sep  7 06:25:23 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/13
Sep  7 06:25:23 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/13
Sep  7 06:25:24 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/13
Sep  7 06:25:24 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/13
Sep  7 06:25:24 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/13
Sep  7 06:25:25 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/13
Sep  7 06:25:25 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/13
Sep  7 06:25:25 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/13
```

```
Sep  7 06:25:28 PIXName %PIX-7-609001: Built local-host db:10.0.0.1
Sep  7 06:25:28 PIXName %PIX-6-302013: Built inbound TCP connection 141968 for db:10.0.0.1/60749 (10
Sep  7 06:25:28 PIXName %PIX-7-710002: TCP access permitted from 10.0.0.1/60749 to db:10.0.0.2/ssh
Sep  7 06:26:20 PIXName %PIX-5-304001: 203.87.123.139 Accessed URL 10.0.0.10:/Home/index.cfm
Sep  7 06:26:20 PIXName %PIX-5-304001: 203.87.123.139 Accessed URL 10.0.0.10:/aboutus/volunteers.cfm
Sep  7 06:26:49 PIXName %PIX-4-106023: Deny udp src outside:204.16.208.49/58939 dst dmz:10.0.0.158/10
Sep  7 06:26:49 PIXName %PIX-4-106023: Deny udp src outside: 204.16.208.49/58940 dst dmz:10.0.0.158/1
Sep  7 06:31:26 PIXName %PIX-7-711002: Task ran for 330 msec, Process= ssh_init, PC = fddd93, Traceba
Sep  7 06:31:32 PIXName %PIX-6-315011: SSH session from 10.0.0.254 on interface db for user "" discon

%PIX-7-710001: TCP access requested from 192.168.2.10/13269 to outside:192.168.2.14/ssh
%PIX-7-710001: TCP access requested from 192.168.2.10/13528 to outside:192.168.2.14/ssh
%PIX-7-710001: TCP access requested from 192.168.2.10/14154 to outside:192.168.2.14/ssh
%PIX-7-710001: TCP access requested from 192.168.2.10/19067 to outside:192.168.2.14/ssh
%PIX-7-710001: TCP access requested from 192.168.2.10/21532 to outside:192.168.2.14/ssh
%PIX-7-710001: TCP access requested from 192.168.2.10/27167 to outside:192.168.2.14/ssh
%PIX-7-710001: TCP access requested from 192.168.2.10/29488 to outside:192.168.2.14/ssh
%PIX-7-710001: TCP access requested from 192.168.2.10/32597 to outside:192.168.2.14/ssh
%PIX-7-710001: TCP access requested from 192.168.2.10/40654 to outside:192.168.2.14/ssh
%PIX-7-710001: TCP access requested from 192.168.2.10/48798 to outside:192.168.2.14/ssh
%PIX-7-710001: TCP access requested from 192.168.2.10/7180 to outside:192.168.2.14/ssh
%PIX-7-710002: TCP access permitted from 192.168.2.10/13269 to outside:192.168.2.14/ssh
%PIX-7-710002: TCP access permitted from 192.168.2.10/13528 to outside:192.168.2.14/ssh
%PIX-7-710002: TCP access permitted from 192.168.2.10/14154 to outside:192.168.2.14/ssh
%PIX-7-710002: TCP access permitted from 192.168.2.10/19067 to outside:192.168.2.14/ssh
%PIX-7-710002: TCP access permitted from 192.168.2.10/21532 to outside:192.168.2.14/ssh
%PIX-7-710002: TCP access permitted from 192.168.2.10/27167 to outside:192.168.2.14/ssh
%PIX-7-710002: TCP access permitted from 192.168.2.10/29488 to outside:192.168.2.14/ssh
%PIX-7-710002: TCP access permitted from 192.168.2.10/32597 to outside:192.168.2.14/ssh
%PIX-7-710002: TCP access permitted from 192.168.2.10/40654 to outside:192.168.2.14/ssh
%PIX-7-710002: TCP access permitted from 192.168.2.10/48798 to outside:192.168.2.14/ssh
%PIX-7-710002: TCP access permitted from 192.168.2.10/7180 to outside:192.168.2.14/ssh
%PIX-7-710005: UDP request discarded from 0.0.0.0/68 to outside:255.255.255.255/bootps
%PIX-7-710005: UDP request discarded from 192.168.1.2/137 to inside:192.168.1.255/netbios-ns
%PIX-7-710005: UDP request discarded from 192.168.1.2/138 to inside:192.168.1.255/netbios-dgm
%PIX-7-710005: UDP request discarded from 192.168.1.2/3935 to inside:192.168.1.1/1900
%PIX-7-710005: UDP request discarded from 192.168.2.1/137 to outside:192.168.2.11/netbios-ns
%PIX-7-710005: UDP request discarded from 192.168.2.1/137 to outside:192.168.2.14/netbios-ns
%PIX-7-710005: UDP request discarded from 192.168.2.11/137 to outside:192.168.2.255/netbios-ns
%PIX-7-710005: UDP request discarded from 192.168.2.11/138 to outside:192.168.2.255/netbios-dgm
%PIX-7-710005: UDP request discarded from 192.168.2.11/68 to outside:255.255.255.255/bootps
%PIX-7-710005: UDP request discarded from 192.168.2.12/137 to outside:192.168.2.255/netbios-ns
%PIX-7-710005: UDP request discarded from 192.168.2.12/138 to outside:192.168.2.255/netbios-dgm
%PIX-7-710005: UDP request discarded from 192.168.2.12/68 to outside:255.255.255.255/bootps
%PIX-7-710005: UDP request discarded from 192.168.2.13/137 to outside:192.168.2.255/netbios-ns
%PIX-7-710005: UDP request discarded from 192.168.2.13/138 to outside:192.168.2.255/netbios-dgm
%PIX-7-710005: UDP request discarded from 192.168.2.13/68 to outside:255.255.255.255/bootps
%PIX-7-710005: UDP request discarded from 192.168.2.190/137 to outside:192.168.2.255/netbios-ns
%PIX-6-315011: SSH session from 192.168.2.10 on interface outside for user "roo" disconnected by SSH
%PIX-6-604101: DHCP client interface outside: Allocated ip = 192.168.2.11, mask = 255.255.255.0, gw =
%PIX-6-604101: DHCP client interface outside: Allocated ip = 192.168.2.14, mask = 255.255.255.0, gw =
%PIX-6-604103: DHCP daemon interface inside:  address granted 000c.29e4.ebc3 (12.168.1.3)
%PIX-6-604103: DHCP daemon interface inside:  address granted 000c.29e4.ebc3 (12.168.1.4)
%PIX-6-604103: DHCP daemon interface inside:  address granted 0100.0d9d.8283.ec(192.168.1.2)
%PIX-6-605004: Login denied from 192.168.2.10/13269 to outside:192.168.2.14/ssh for user "root"
%PIX-6-605004: Login denied from 192.168.2.10/13528 to outside:192.168.2.14/ssh for user "dcid"
%PIX-6-605004: Login denied from 192.168.2.10/14154 to outside:192.168.2.14/ssh for user "root"
%PIX-3-305006: portmap translation creation failed for tcp src inside:192.168.1.2/2893 dst outside:19
```

```
%PIX-3-305006: portmap translation creation failed for tcp src inside:192.168.1.2/2892 dst outside:19
%PIX-3-201008: The PIX is disallowing new connections.
%PIX-3-106011: Deny inbound (No xlate) udp src outside:192.168.2.1/137 dst outside:192.168.2.14/137
%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.245.209.21/80 dst outside:192.168.2.14/1823
%PIX-3-106011: Deny inbound (No xlate) tcp src outside:195.27.11.150/80 dst outside:192.168.2.14/1717
%PIX-3-106011: Deny inbound (No xlate) tcp src outside:195.27.11.150/80 dst outside:192.168.2.14/1716
%PIX-3-106011: Deny inbound (No xlate) tcp src outside:195.27.11.143/80 dst outside:192.168.2.14/1721
%PIX-3-106011: Deny inbound (No xlate) tcp src outside:195.27.11.142/80 dst outside:192.168.2.14/1720

%PIX-3-106011: Deny inbound (No xlate) tcp src inside:10.100.7.43/80 dst inside:10.100.4.71/2285
%PIX-3-106011: Deny inbound (No xlate) tcp src inside:10.100.5.43/80 dst inside:10.100.4.71/2285
%PIX-3-106011: Deny inbound (No xlate) tcp src outside:213.98.202.19/3959 dst outside:213.58.100.132/
%PIX-3-106011: Deny inbound (No xlate) tcp src outside:213.98.202.19/3959 dst outside:213.58.100.132/
%PIX-3-106011: Deny inbound (No xlate) udp src outside:192.168.2.1/137 dst outside:192.168.2.14/137
%PIX-3-106010: Deny inbound tcp src outside:213.98.79.233/2620 dst dmz:213.98.254.145/135
%PIX-3-106010: Deny inbound tcp src outside:213.91.69.233/2620 dst dmz:213.98.254.145/145

Jan 28 02:04:30 pix-inside %PIX-3-106010: Deny inbound tcp src outside:67.200.184.237/1262 dst inside
Jan 28 02:01:08 pix-inside %PIX-3-106010: Deny inbound udp src outside:216.143.1.229/1321 dst inside
Jan 28 06:17:47 pix-inside %PIX-3-106010: Deny inbound icmp src outside:80.181.210.80 dst inside:10.1
Jan 28 00:21:50 pix-inside %PIX-3-106011: Deny inbound (No xlate) tcp src outside:217.228.221.121/123
Jan 28 00:01:38 pix-inside %PIX-4-106023: Deny tcp src outside:213.22.40.190/1381 dst inside:10.107.8
Jan 28 00:01:38 pix-inside %PIX-4-106023: Deny udp src outside:24.200.88.234/1025 dst inside:10.107.3
Jan 28 00:41:42 pix-inside %PIX-4-106023: Deny icmp src outside:128.9.160.165 dst inside:10.107.19.10
Jan 28 01:48:01 pix-inside %PIX-4-106023: Deny protocol 4 src outside:131.119.0.197 dst inside:10.107

<164>Jul 05 2004 00:58:00: %PIX-4-400011: IDS:2001 ICMP unreachable from 172.54.32.18 to 192.168.54.2
<162>Jul 05 2004 00:56:23: %PIX-2-109011: Authen Session Start: user 'Graffe', sid 55
<164>Jul 05 2004 00:56:26: %PIX-4-500004: Invalid transport field for protocol=17, from 10.34.55.198/
<164>Dec 05 2006 12:06:59: %PIX-4-405001: Received ARP request collision from 10.54.100.218/007e.0cfe
```

Alert Messages, Severity 1:

Critical Messages, Severity 2:

```
%PIX-2-106006: Deny inbound UDP from ***/20031 to ***/20031 on  interface vpn
%PIX-2-106006: Deny inbound UDP from ***/20031 to ***/20031 on  interface vpn
%PIX-2-106006: Deny inbound UDP from ***/54481 to ***/1026 on  interface vpn
%PIX-2-106006: Deny inbound UDP from ***9/20031 to ***/20031 on interface vpn
%PIX-2-106006: Deny inbound UDP from ***/20031 to ***/20031 on  interface vpn
```

Error Messages, Severity 3:

```
%PIX-3-313001: Denied ICMP type=11, code=0 from 192.168.30.2 on interface 2
```

Warning Messages, Severity 4:

```
%PIX-4-410001: Dropped UDP DNS reply from os-to-dmz:192.168.30.2 to outside:192.168.100.2/53; packet
```

Notification Messages, Severity 5:

```
%PIX-5-304001: 192.168.20.50 Accessed URL x.y.z.a:/test/xx/yy.html
```

Informational Messages, Severity 6:

```
%PIX-6-302016: Teardown UDP connection 1042068 for outside:192.168.20.45/53 to inside:192.168.20.208/
%PIX-6-106015: Deny TCP (no connection) from 192.168.2.50/443 to 192.168.20/65 flags RST on interface
```

Debugging Messages, Severity 7:

```
%PIX-7-710005: UDP request discarded from  192.168.20.45/53 to outside:192.168.20.208/37989
```

Cisco Secure ACS

Cisco Secure ACS is an access control server which can be used for centralized authentication, authorization and accounting. The log files from this product can be very useful in security analysis and correlation.

Information about the logging facilities in the Windows version of the product (version 3.2) can be found here.

Here is a sample of the log file tracking failed login attempts : filename = Failed Attempt 2004-05-18.csv

```
Date,Time,Message-Type,User-Name,Group-Name,Caller-ID,Authen-Failure-Code,Author-Failure-Code,Author-
05/18/2004,02:11:03,Authen failed,bscorpio,punks,122.55.32.13,External DB user invalid or bad passwor
05/18/2004,02:11:31,Authen failed,bscorpio,punks,122.55.32.13,External DB user invalid or bad passwor
05/18/2004,02:12:40,Authen failed,bscorpio,punks,122.55.32.13,External DB user invalid or bad passwor
05/18/2004,02:12:50,Authen failed,bscorpio,punks,122.55.32.13,External DB user invalid or bad passwor
05/18/2004,02:13:00,Authen failed,bscorpio,punks,122.55.32.13,Windows password change failed,,,19,10
05/18/2004,02:13:31,Authen failed,bscorpio,punks,122.55.32.13,External DB user invalid or bad passwor
05/18/2004,02:13:41,Authen failed,bscorpio,punks,122.55.32.13,External DB user invalid or bad passwor
05/18/2004,02:14:16,Authen failed,bscorpio,punks,122.55.32.13,External DB user invalid or bad passwor
05/18/2004,02:14:37,Authen failed,bscorpio,punks,122.55.32.13,External DB user invalid or bad passwor
05/18/2004,02:15:15,Authen failed,bscorpio,punks,122.55.32.13,External DB user invalid or bad passwor
05/18/2004,08:14:32,Authen failed,bscorpio,punks,122.55.32.35,External DB user invalid or bad passwor
```

Here is a sample of the log file tracking successful logins : filename = Passed Authentications 2004-07-08.csv

Date,Time,Message-Type,User-Name,Group-Name,Caller-ID,NAS-Port,NAS-IP-Address 07/08/2004,08:13:54,Authen OK,bplack,punks,198.47.27.99,106,10.27.3.1 07/08/2004,08:19:17,Authen OK,bplack,punks,198.47.27.99,107,10.27.3.1 07/08/2004,08:24:21,Authen OK,bplack,punks,198.47.27.99,108,10.27.3.1 07/08/2004,08:31:17,Authen OK,bplack,punks,198.47.27.99,109,10.27.3.1 07/08/2004,10:25:32,Authen OK,Dandre,punks,198.47.27.99,110,10.27.3.1 07/08/2004,11:12:23,Authen OK,bplack,punks,198.47.27.99,111,10.27.3.1 07/08/2004,11:15:59,Authen OK,bplack,punks,198.47.27.99,113,10.27.3.1 07/08/2004,11:27:31,Authen OK,bplack,punks,198.47.27.99,114,10.27.3.1 07/08/2004,11:38:25,Authen OK,bplack,punks,198.47.27.99,115,10.27.3.1 07/08/2004,11:39:38,Authen OK,bplack,punks,198.47.27.99,116,10.27.3.1 07/08/2004,13:15:08,Authen OK,bplack,punks,198.47.27.99,117,10.27.3.1 07/08/2004,14:29:25,Authen OK,bplack,punks,198.47.27.99,118,10.27.3.1 07/08/2004,14:47:56,Authen OK,bplack,punks,198.47.27.99,119,10.27.3.1 07/08/2004,14:54:39,Authen OK,bretuwu,punks,198.47.27.99,120,10.27.3.1

The log files are stored in CSV (comma delimited).

These samples were taken from the Cisco Secure ACS version 3.2 for Windows

Log Samples for MySQL

Notes:

The timestamp of MySQL logs only appear in the first event during that time. It means that <br /> if you have two logs within the same second, only the first one will have the timestamp.

Startup:

```
060516 22:38:46  mysqld started
InnoDB: The first specified data file ./ibdata1 did not exist:
InnoDB: a new database to be created!
060516 22:38:54  InnoDB: Started; log sequence number 0 0
```

Shutdown:

```
060516 22:38:54  mysqld ended
070823 20:58:09 [Note] /usr/libexec/mysqld: Shutdown complete
```

Error:

```
060516 22:38:54 [ERROR] Fatal error: Can't open privilege tables: Table 'mysql.host' doesn't exist
```

Connections,queries:

```
070823 21:00:32       1 Connect     root@localhost on test1
070823 21:00:48       1 Query       show tables
070823 21:00:56       1 Query       select * from category
070917 16:29:01      21 Query       select * from location
070917 16:29:12      21 Query       select * from location where id = 1 LIMIT 1
```

Log Samples for PostgreSQL

Login/Logout:

```
[2007-08-31 19:22:21.469 ADT] :[unknown] LOG:  connection received: host=192.168.2.99 port=52136
[2007-08-31 19:22:21.485 ADT] 192.168.2.99:ossecdb LOG:  connection authorized: user=ossec_user datab
[2007-08-31 19:22:22.427 ADT] 192.168.2.99:ossecdb LOG:  disconnection: session time: 0:00:00.95 user
[2007-09-27 11:02:44.941 ADT] 192.168.2.10:ossecdb ERROR:  relation "lala" does not exist
[2007-09-27 11:02:46.444 ADT] 192.168.2.10:ossecdb LOG:  disconnection: session time: 0:00:35.79 user
```

Log messages:

```
[2007-09-01 07:14:41.062 ADT] : LOG:  autovacuum: processing database "template1"
[2007-09-01 07:15:41.079 ADT] : LOG:  autovacuum: processing database "ossecdb"
```

Query log:

```
[2007-09-01 16:44:49.244 ADT] 192.168.2.10:ossecdb LOG:  duration: 4.550 ms  statement: SELECT id FRO
[2007-09-01 16:44:49.251 ADT] 192.168.2.10:ossecdb LOG:  duration: 5.252 ms  statement: INSERT INTO l
[2007-09-01 16:44:49.252 ADT] 192.168.2.10:ossecdb LOG:  duration: 0.016 ms  statement: SELECT id FRO
[2007-09-27 11:02:51.611 ADT] 192.168.2.10:ossecdb LOG:  statement: INSERT INTO alert(id,server_id,ru
```

Query error:

```
[2007-08-31 19:17:42.128 ADT] 192.168.2.99:test ERROR:  relation "alertaaa" does not exist
[2007-08-31 19:17:46.375 ADT] 192.168.2.99:test ERROR:  syntax error at or near "a" at character 1
[2007-09-27 11:02:44.941 ADT] 192.168.2.10:ossecdb ERROR:  relation "lala" does not exist
```

Authentication error:

```
[2007-09-01 19:08:49.862 ADT] : LOG:  connection received: host=192.168.2.99 port=37142
[2007-09-01 19:08:49.869 ADT] 192.168.2.99: FATAL:  password authentication failed for user "ossec_us
```

Log Samples from PHP

php-cgi log:

```
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  Module 'gd' already loaded in Unknown on line 0
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  PHP Startup: Unable to load dynamic library '/usr/lib/ph
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  PHP Startup: Unable to load dynamic library '/usr/lib/ph
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  PHP Startup: Unable to load dynamic library '/usr/lib/ph
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  Module 'ADOdb' already loaded in Unknown on line 0
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  Module 'gd' already loaded in Unknown on line 0
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  Module 'ADOdb' already loaded in Unknown on line 0
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  Module 'gd' already loaded in Unknown on line 0
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  Module 'gd' already loaded in Unknown on line 0
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  PHP Startup: Unable to load dynamic library '/usr/lib/ph
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  Module 'mysql' already loaded in Unknown on line 0
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  Module 'mysqli' already loaded in Unknown on line 0
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  PHP Startup: Unable to load dynamic library '/usr/lib/ph
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  PHP Startup: Unable to load dynamic library '/usr/lib/ph
Jan 28 21:56:25 Lab12 php-cgi: PHP Warning:  Cannot load module 'pdo_sqlite' because required module
```

Urlscan Log samples

Taken From log example posted here

Log Samples from Named

Some information about named logs can be found at:

http://www.netadmintools.com/art233.html List of errors List of Bind 8 and 9 errors

Query cache denied (attempt to use server not authorized):

```
Aug 29 15:33:13 ns3 named[464]: client 217.148.39.3#1036: query (cache) denied
Aug 29 15:33:13 ns3 named[464]: client 217.148.39.4#32769: query (cache) denied
Aug 29 15:33:13 ns3 named[464]: client 217.148.39.3#1036: query (cache) denied
Aug 29 15:33:13 ns3 named[464]: client 217.148.39.4#32769: query (cache) denied
```

Fatal errors:

```
named[17546]: loading configuration: failure
named[17546]: exiting (due to fatal error)
```

Zone transfer errors:

```
Jul  4 10:31:39 internet-gw named[7136]: zone dominio.com.br/IN/external: expired
```

Log samples for Checkpoint

Sample 1:

..code-block:: console

Apr 11 11:04:48 hostng Checkpoint: 21Aug2007 12:00:00 accept 10.10.10.2 >eth0 rule: 100; rule_uid: {00000000-0000-0000-0000-000000000000}; service_id: nbdatagram; src: 10.10.10.3; dst: 10.10.10.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138;

Sample 2:

Sep 3 15:10:54 192.168.99.1 Checkpoint: 3Sep2007 15:10:28 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 200.14.120.9; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32769; Sep 3 15:10:54 192.168.99.1 Checkpoint: 3Sep2007 15:10:28 accept 192.168.99.1 >eth5 rule: 33; rule_uid: {AAAAAAAA-9999-8888-F33256AF77FB}; service_id: lotus; src: 192.168.11.131; dst: 192.168.99.13; proto: tcp; product: VPN-1 & FireWall-1; service: 1352; s_port: 2555; Sep 3 15:10:54 192.168.99.1 Checkpoint: 3Sep2007 15:10:28 accept 192.168.99.1 >eth5 rule: 33; rule_uid: {AAAAAAAA-9999-8888-F33256AF77FB}; service_id: lotus; src: 192.168.11.131; dst: 192.168.99.13; proto: tcp; product: VPN-1 & FireWall-1; service: 1352; s_port: 2556; Sep 3 15:10:54 192.168.99.1 Checkpoint: 3Sep2007 15:10:29 accept 192.168.99.1 >eth5 rule: 112; rule_uid: {11111111-2222-3333-97BB-2362F0B7F576}; service_id: icmp-proto; ICMP: Echo Request; src: 192.168.11.131; dst: 192.168.99.10; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:10:54 192.168.99.1 Checkpoint: 3Sep2007 15:10:35 accept 192.168.99.1 >eth2 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.13.10; dst: 192.168.200.2; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:10:54 192.168.99.1 Checkpoint: 3Sep2007 15:10:35 accept 192.168.99.1 >eth2 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.13.10; dst: 192.168.99.10; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:10:54 192.168.99.1 Checkpoint: 3Sep2007 15:12:04 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbdatagram; src: 192.168.11.131; dst: 192.168.11.255; proto: udp; product: VPN-1 &

FireWall-1; service: 138; s_port: 138; Sep 3 15:10:54 192.168.99.1 Checkpoint: 3Sep2007 15:12:08 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 4.23.34.126; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2854; Sep 3 15:10:54 192.168.99.1 Checkpoint: 3Sep2007 15:10:49 accept 192.168.99.1 >eth5 rule: 112; rule_uid: {11111111-2222-3333-97BB-2362F0B7F576}; service_id: icmp-proto; ICMP: Echo Request; src: 192.168.11.200; dst: 192.168.99.10; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:10:54 192.168.99.1 Checkpoint: 3Sep2007 15:10:52 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; dst: 255.255.255.255; proto: udp; product: VPN-1 & FireWall-1; service: 67; s_port: 68; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:10:54 accept 192.168.99.1 >eth8 rule: 132; rule_uid: {11111111-2222-3333-80CE-68F956E049EE}; service_id: icmp-proto; ICMP: Echo Request; src: 192.168.99.226; dst: 192.168.11.200; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:10:54 accept 192.168.99.1 >eth8 rule: 132; rule_uid: {11111111-2222-3333-80CE-68F956E049EE}; service_id: microsoft-ds; src: 192.168.99.226; dst: 192.168.11.200; proto: tcp; product: VPN-1 & FireWall-1; service: 445; s_port: 1726; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:10:54 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.99.185; dst: 192.149.252.44; proto: tcp; product: VPN-1 & FireWall-1; service: 43; s_port: 57172; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:10:54 accept 192.168.99.1 >eth5 rule: 112; rule_uid: {11111111-2222-3333-97BB-2362F0B7F576}; service_id: icmp-proto; ICMP: Echo Request; src: 192.168.11.200; dst: 192.168.99.226; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:10:56 accept 192.168.99.1 >eth5 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.0.254; dst: 192.168.11.3; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:12:24 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbname; src: 192.168.11.200; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 137; s_port: 137; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:12:24 drop 192.168.11.7 >eth5 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 172.18.40.250; dst: 172.18.40.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:11:00 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 148.160.29.6; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 33120; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:12:29 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 8.255.17.254; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2855; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:11:08 accept 192.168.99.1 >eth2 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.13.3; dst: 192.168.200.2; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:11:15 drop 192.168.99.1 >eth5 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.0.180; dst: 192.168.0.255; proto: udp; product: VPN-1 & FireWall-1; service: 137; s_port: 137; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:11:16 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 64.243.236.3; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 46485; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:12:49 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbdatagram; src: 192.168.11.35; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:12:50 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 204.160.122.126; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2856; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:11:25 accept 192.168.99.1 >eth2 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.13.3; dst: 192.168.99.10; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:12:53 accept 192.168.11.7 >eth8 rule: 27; rule_uid: {33333333-2222-1111-

A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.11.99; dst: 218.185.224.7; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 4538; Sep 3 15:11:40 192.168.99.1 Checkpoint: 3Sep2007 15:11:29 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 216.230.128.228; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 50268; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:11:41 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.99.195; dst: 192.168.56.10; proto: tcp; product: VPN-1 & FireWall-1; service: 3013; s_port: 1352; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:13:11 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 4.23.34.126; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2857; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:11:45 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 202.134.1.10; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 1061; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:11:49 accept 192.168.99.1 >eth8 rule: 132; rule_uid: {11111111-2222-3333-80CE-68F956E049EE}; service_id: icmp-proto; ICMP: Echo Request; src: 192.168.99.228; dst: 192.168.11.200; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:11:49 accept 192.168.99.1 >eth8 rule: 132; rule_uid: {11111111-2222-3333-80CE-68F956E049EE}; service_id: microsoft-ds; src: 192.168.99.228; dst: 192.168.11.200; proto: tcp; product: VPN-1 & FireWall-1; service: 445; s_port: 1434; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:11:54 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; dst: 255.255.255.255; proto: udp; product: VPN-1 & FireWall-1; service: 67; s_port: 68; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:11:54 accept 192.168.99.1 >eth8 rule: 40; rule_uid: {33333333-2222-1111-C048F9B6D5DA}; service_id: smtp; src: 192.168.99.185; dst: 192.168.13.18; proto: tcp; product: VPN-1 & FireWall-1; service: 25; s_port: 39250; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:13:22 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbdatagram; src: 192.168.11.116; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:11:57 accept 192.168.99.1 >eth5 rule: 33; rule_uid: {AAAAAAAA-9999-8888-F33256AF77FB}; service_id: lotus; src: 192.168.11.115; dst: 192.168.99.13; proto: tcp; product: VPN-1 & FireWall-1; service: 1352; s_port: 3084; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:12:00 accept 192.168.99.1 >eth8 rule: 132; rule_uid: {11111111-2222-3333-80CE-68F956E049EE}; service_id: icmp-proto; ICMP: Echo Request; src: 192.168.99.47; dst: 192.168.11.200; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:12:00 accept 192.168.99.1 >eth8 rule: 132; rule_uid: {11111111-2222-3333-80CE-68F956E049EE}; service_id: microsoft-ds; src: 192.168.99.47; dst: 192.168.11.200; proto: tcp; product: VPN-1 & FireWall-1; service: 445; s_port: 1268; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:12:00 accept 192.168.99.1 >eth8 rule: 132; rule_uid: {11111111-2222-3333-80CE-68F956E049EE}; service_id: nbsession; src: 192.168.99.47; dst: 192.168.11.200; proto: tcp; product: VPN-1 & FireWall-1; service: 139; s_port: 1269; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:12:04 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.99.185; dst: 199.43.0.144; proto: tcp; product: VPN-1 & FireWall-1; service: 43; s_port: 47703; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:13:32 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 8.255.17.254; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2858; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:12:05 accept 192.168.99.1 >eth5 rule: 33; rule_uid: {AAAAAAAA-9999-8888-F33256AF77FB}; service_id: lotus; src: 192.168.11.131; dst: 192.168.99.13; proto: tcp; product: VPN-1 & FireWall-1; service: 1352; s_port: 2568; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:12:05 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 209.244.7.35; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 5304; Sep 3 15:12:20 192.168.99.1 Checkpoint: 3Sep2007 15:13:48 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbname; src: 192.168.11.33; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 137; s_port: 137; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:12:22 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-

2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 200.75.51.132; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 33504; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:13:53 drop 192.168.11.7 >eth2 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; ICMP: Echo Request; src: 203.193.149.227; dst: 64.129.8.245; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:13:53 drop 192.168.11.7 >eth2 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; ICMP: Echo Request; src: 203.193.149.227; dst: 64.129.8.246; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:13:53 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 204.160.122.126; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2859; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:12:29 accept 192.168.99.1 >eth2 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.13.3; dst: 192.168.99.10; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:12:31 accept 192.168.99.1 >eth5 rule: 106; rule_uid: {33333333-2222-1111-F25776101B8B}; rule_name: VOIP?; service_id: SAV-Intel-PDS; src: 192.168.11.117; dst: 192.168.99.10; proto: udp; product: VPN-1 & FireWall-1; service: 38293; s_port: 1061; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:12:36 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 148.160.29.6; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 33120; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:14:05 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbdatagram; src: 192.168.11.200; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:14:05 drop 192.168.11.7 >eth2 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; ICMP: Echo Request; src: 203.193.149.227; dst: 64.129.8.249; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:12:45 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 213.51.144.168; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 5353; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:14:12 accept 192.168.11.7 >eth8 rule: 114; rule_uid: {33333333-2222-1111-7E7A07E3B187}; service_id: http; src: 192.168.11.154; dst: 216.239.51.91; proto: tcp; xlatesrc: 64.128.3.58; NAT_rulenum: 7; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 57720; xlatesport: 30022; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:14:12 drop 192.168.11.8 >eth2 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 61.153.230.18; dst: 64.128.3.60; proto: udp; product: VPN-1 & FireWall-1; service: 1434; s_port: 1112; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:14:14 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 8.255.17.254; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2861; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:14:21 drop 192.168.11.7 >eth5 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 172.18.40.250; dst: 172.18.40.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:14:24 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; src: 192.168.11.154; dst: 209.85.199.109; proto: tcp; xlatesrc: 64.128.3.58; NAT_rulenum: 7; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 995; s_port: 57722; xlatesport: 30023; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:14:24 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; src: 192.168.11.154; dst: 209.85.199.109; proto: tcp; xlatesrc: 64.128.3.58; NAT_rulenum: 7; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 995; s_port: 57723; xlatesport: 30024; Sep 3 15:12:56 192.168.99.1 Checkpoint: 3Sep2007 15:14:24 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; src: 192.168.11.154; dst: 209.85.199.109; proto: tcp; xlatesrc: 64.128.3.58; NAT_rulenum: 7; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 995; s_port: 57724; xlatesport: 30025; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:14:25 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; src: 192.168.11.154; dst: 209.85.199.109; proto: tcp; xlatesrc: 64.128.3.58; NAT_rulenum: 7; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 995; s_port: 57725;

xlatesport: 30026; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:14:26 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; src: 192.168.11.154; dst: 209.85.199.109; proto: tcp; xlatesrc: 64.128.3.58; NAT_rulenum: 7; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 995; s_port: 57726; xlatesport: 30027; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:12:57 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; dst: 255.255.255.255; proto: udp; product: VPN-1 & FireWall-1; service: 67; s_port: 68; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:14:26 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; src: 192.168.11.154; dst: 209.85.199.109; proto: tcp; xlatesrc: 64.128.3.58; NAT_rulenum: 7; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 995; s_port: 57727; xlatesport: 30028; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:14:30 accept 192.168.11.7 >eth8 rule: 114; rule_uid: {33333333-2222-1111-7E7A07E3B187}; service_id: http; src: 192.168.11.154; dst: 65.55.139.125; proto: tcp; xlatesrc: 64.128.3.58; NAT_rulenum: 7; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 57728; xlatesport: 30029; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:13:03 accept 192.168.99.1 >eth5 rule: 111; rule_uid: {AAAAAAAA-9999-8888-6F8CB5EB44F2}; service_id: CAP; src: 192.168.11.200; dst: 192.168.99.10; proto: tcp; product: VPN-1 & FireWall-1; service: 1026; s_port: 1628; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:13:03 accept 192.168.99.1 >eth5 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.0.254; dst: 192.168.11.3; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:13:03 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 62.145.135.100; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 53; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:13:04 accept 192.168.99.1 >eth8 rule: 40; rule_uid: {33333333-2222-1111-C048F9B6D5DA}; service_id: smtp; src: 192.168.99.185; dst: 192.168.13.18; proto: tcp; product: VPN-1 & FireWall-1; service: 25; s_port: 39259; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:14:35 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 4.23.34.126; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2862; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:13:15 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 202.52.162.40; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 9867; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:13:16 accept 192.168.99.1 >eth2 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.13.3; dst: 192.168.200.2; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:13:17 accept 192.168.99.1 >eth5 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.0.254; dst: 192.168.11.4; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:13:17 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 166.70.31.250; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 1045; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:13:18 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 64.191.208.15; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 55555; Sep 3 15:13:24 192.168.99.1 Checkpoint: 3Sep2007 15:13:19 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 202.108.12.72; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 28585; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:25 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 206.13.28.16; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 54618; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:28 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 160.124.208.1; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 49173; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:28 accept 192.168.99.1 >eth5 rule: 112; rule_uid: {11111111-2222-3333-97BB-2362F0B7F576}; service_id: MS-RPC; src: 192.168.11.119; dst: 192.168.99.10; proto: tcp; product: VPN-1 & FireWall-

1; service: 135; s_port: 4597; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:28 accept 192.168.99.1 >eth5 rule: 111; rule_uid: {AAAAAAAA-9999-8888-6F8CB5EB44F2}; service_id: CAP; src: 192.168.11.119; dst: 192.168.99.10; proto: tcp; product: VPN-1 & FireWall-1; service: 1026; s_port: 4598; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:14:56 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 8.12.217.126; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2863; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:14:58 accept 192.168.11.7 >eth8 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.11.99; dst: 202.71.97.92; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 32242; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:30 accept 192.168.99.1 >eth8 rule: 132; rule_uid: {11111111-2222-3333-80CE-68F956E049EE}; service_id: SAV-Roaming-Clients; src: 192.168.99.10; dst: 192.168.11.159; proto: udp; product: VPN-1 & FireWall-1; service: 2967; s_port: 2967; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:32 accept 192.168.99.1 >eth5 rule: 40; rule_uid: {33333333-2222-1111-C048F9B6D5DA}; service_id: smtp; src: 192.168.11.240; dst: 192.168.13.18; proto: tcp; product: VPN-1 & FireWall-1; service: 25; s_port: 50412; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:33 accept 192.168.99.1 >eth2 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.13.3; dst: 192.168.99.10; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:34 accept 192.168.99.1 >eth8 rule: 132; rule_uid: {11111111-2222-3333-80CE-68F956E049EE}; service_id: MS-RPC; src: 192.168.99.228; dst: 192.168.11.200; proto: tcp; product: VPN-1 & FireWall-1; service: 135; s_port: 1443; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:34 accept 192.168.99.1 >eth8 rule: 132; rule_uid: {11111111-2222-3333-80CE-68F956E049EE}; service_id: Remote_Storm; src: 192.168.99.228; dst: 192.168.11.200; proto: tcp; product: VPN-1 & FireWall-1; service: 1025; s_port: 1444; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:37 accept 192.168.99.1 >eth5 rule: 112; rule_uid: {11111111-2222-3333-97BB-2362F0B7F576}; service_id: icmp-proto; ICMP: Echo Request; src: 192.168.11.141; dst: 192.168.99.10; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:38 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 217.114.163.198; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 54816; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:39 accept 192.168.99.1 >eth8 rule: 132; rule_uid: {11111111-2222-3333-80CE-68F956E049EE}; service_id: SAV-Roaming-Clients; src: 192.168.99.10; dst: 192.168.11.160; proto: udp; product: VPN-1 & FireWall-1; service: 2967; s_port: 2967; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:41 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.99.195; dst: 192.168.56.10; proto: tcp; product: VPN-1 & FireWall-1; service: 3013; s_port: 1352; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:15:14 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbdatagram; src: 192.168.11.34; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138; Sep 3 15:13:48 192.168.99.1 Checkpoint: 3Sep2007 15:13:47 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 212.139.132.22; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 10724; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:13:49 accept 192.168.99.1 >eth5 rule: 112; rule_uid: {11111111-2222-3333-97BB-2362F0B7F576}; src: 192.168.11.141; dst: 192.168.99.10; proto: udp; product: VPN-1 & FireWall-1; service: 389; s_port: 3032; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:13:50 accept 192.168.99.1 >eth5 rule: 112; rule_uid: {11111111-2222-3333-97BB-2362F0B7F576}; src: 192.168.11.141; dst: 192.168.99.10; proto: udp; product: VPN-1 & FireWall-1; service: 389; s_port: 3033; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:13:55 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 198.231.24.101; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 33025; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:13:59 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; dst: 255.255.255.255; proto: udp; product: VPN-1 & FireWall-1; service: 67; s_port: 68; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:14:00 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693};

service_id: domain-udp; src: 195.229.242.132; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32775; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:14:02 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 80.82.99.203; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 4876; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:15:32 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbname; src: 192.168.11.34; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 137; s_port: 137; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:14:06 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 200.23.242.202; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 65397; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:14:06 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 200.23.242.196; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32796; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:15:36 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 72.253.127.9; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2866; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:14:09 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 202.188.0.132; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 62699; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:14:11 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 202.188.0.132; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32822; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:14:12 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 148.160.29.6; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 33120; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:15:40 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbdatagram; src: 192.168.11.113; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:14:14 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.99.185; dst: 192.149.252.44; proto: tcp; product: VPN-1 & FireWall-1; service: 43; s_port: 51922; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:14:22 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 24.92.226.9; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 41255; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:15:57 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 72.253.127.8; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2867; Sep 3 15:14:36 192.168.99.1 Checkpoint: 3Sep2007 15:14:36 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 211.76.137.41; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 36551; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:14:36 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 195.170.2.2; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 44444; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:14:36 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 195.170.0.113; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 44444; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:14:37 accept 192.168.99.1 >eth2 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.13.3; dst: 192.168.99.10; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:16:06 accept 192.168.11.7 >eth8 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.11.99; dst: 193.225.14.161; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 2432; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:16:09 accept 192.168.11.7 >eth8 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.11.99; dst: 141.82.30.252; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 17335; Sep 3 15:15:14 192.168.99.1 Check-

point: 3Sep2007 15:14:49 accept 192.168.99.1 >eth5 rule: 111; rule_uid: {AAAAAAAA-9999-8888-6F8CB5EB44F2}; service_id: CAP; src: 192.168.11.200; dst: 192.168.99.10; proto: tcp; product: VPN-1 & FireWall-1; service: 1026; s_port: 1633; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:14:50 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 24.172.50.197; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32775; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:16:18 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 72.253.127.9; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2869; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:15:02 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; dst: 255.255.255.255; proto: udp; product: VPN-1 & FireWall-1; service: 67; s_port: 68; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:16:33 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbdatagram; src: 192.168.11.112; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:15:06 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.99.183; dst: 192.168.13.19; proto: udp; product: VPN-1 & FireWall-1; service: 161; s_port: 35054; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:15:11 drop 192.168.99.1 >eth5 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.200.11; dst: 192.168.99.186; proto: udp; product: VPN-1 & FireWall-1; service: 162; s_port: 161; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:15:11 drop 192.168.99.1 >eth5 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.200.11; dst: 192.168.99.186; proto: udp; product: VPN-1 & FireWall-1; service: 514; s_port: 514; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:15:11 accept 192.168.99.1 >eth5 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.0.254; dst: 192.168.11.3; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:16:39 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbname; src: 192.168.11.33; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 137; s_port: 137; Sep 3 15:15:14 192.168.99.1 Checkpoint: 3Sep2007 15:16:39 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 72.253.127.8; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2870; Sep 3 15:15:15 192.168.99.1 Checkpoint: 3Sep2007 15:15:14 accept 192.168.99.1 >eth8 rule: 40; rule_uid: {33333333-2222-1111-C048F9B6D5DA}; service_id: smtp; src: 192.168.99.185; dst: 192.168.13.18; proto: tcp; product: VPN-1 & FireWall-1; service: 25; s_port: 39268; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:15 drop 192.168.99.1 >eth5 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.200.12; dst: 192.168.99.186; proto: udp; product: VPN-1 & FireWall-1; service: 514; s_port: 514; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:15 drop 192.168.99.1 >eth5 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.200.12; dst: 192.168.99.186; proto: udp; product: VPN-1 & FireWall-1; service: 162; s_port: 161; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:17 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 64.102.255.43; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 53; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:19 accept 192.168.99.1 >eth5 rule: 112; rule_uid: {11111111-2222-3333-97BB-2362F0B7F576}; service_id: icmp-proto; ICMP: Echo Request; src: 192.168.11.114; dst: 192.168.99.10; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:19 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.99.185; dst: 199.43.0.144; proto: tcp; product: VPN-1 & FireWall-1; service: 43; s_port: 47721; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:20 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 24.94.163.100; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32784; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:21 accept 192.168.99.1 >eth8 rule: 132; rule_uid: {11111111-2222-3333-80CE-68F956E049EE}; service_id: snmp; src: 192.168.99.183; dst: 192.168.11.20; proto: udp; product: VPN-1 & FireWall-1; service: 161; s_port: 35137; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:16:58 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-

09283F665349}; service_id: nbdatagram; src: 192.168.11.114; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:31 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 87.86.189.66; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32769; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:17:00 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 72.253.127.9; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2872; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:39 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 69.50.181.10; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 3372; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:40 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 211.99.188.37; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32769; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:41 accept 192.168.99.1 >eth2 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.13.3; dst: 192.168.99.10; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:41 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.99.195; dst: 192.168.56.10; proto: tcp; product: VPN-1 & FireWall-1; service: 3013; s_port: 1352; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:48 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 148.160.29.6; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 33120; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:15:49 accept 192.168.99.1 >eth5 rule: 112; rule_uid: {11111111-2222-3333-97BB-2362F0B7F576}; service_id: icmp-proto; ICMP: Echo Request; src: 192.168.11.200; dst: 192.168.99.10; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:15:56 192.168.99.1 Checkpoint: 3Sep2007 15:17:21 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 72.253.127.8; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2873; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:15:58 accept 192.168.99.1 >eth5 rule: 112; rule_uid: {11111111-2222-3333-97BB-2362F0B7F576}; service_id: icmp-proto; ICMP: Echo Request; src: 192.168.11.130; dst: 192.168.99.10; proto: icmp; ICMP Type: 8; ICMP Code: 0; product: VPN-1 & FireWall-1; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:17:26 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbdatagram; src: 192.168.11.36; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:16:02 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 67.18.92.158; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 57903; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:16:04 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; dst: 255.255.255.255; proto: udp; product: VPN-1 & FireWall-1; service: 67; s_port: 68; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:16:05 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 61.8.0.101; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 33217; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:17:38 accept 192.168.11.7 >eth8 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.11.99; dst: 216.135.38.249; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 5862; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:16:13 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 68.87.85.99; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32788; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:16:14 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 217.116.0.179; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 53; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:17:43 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 72.253.127.8; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2875; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:16:16 accept 192.168.99.1

>eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 200.28.4.129; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32000; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:16:17 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41207; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:16:17 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41208; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:17:46 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41207; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:17:46 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41208; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:17:47 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48028; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:16:19 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.99.185; dst: 192.149.252.44; proto: tcp; product: VPN-1 & FireWall-1; service: 43; s_port: 51932; Sep 3 15:16:22 192.168.99.1 Checkpoint: 3Sep2007 15:16:19 accept 192.168.99.1 >eth8 rule: 40; rule_uid: {33333333-2222-1111-C048F9B6D5DA}; service_id: smtp; src: 192.168.99.185; dst: 192.168.13.18; proto: tcp; product: VPN-1 & FireWall-1; service: 25; s_port: 39278; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:16:23 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 150.63.3.240; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 47343; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:17:51 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 47925; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:17:51 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: https; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 443; s_port: 47903; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:17:52 drop 192.168.11.8 >eth2 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 58.20.228.52; dst: 64.128.3.60; proto: udp; product: VPN-1 & FireWall-1; service: 1434; s_port: 3479; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:16:29 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41209; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:16:29 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41210; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:17:58 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41209; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:17:59 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41210; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:18:02 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 47997; Sep 3 15:16:42 192.168.99.1 Check-

point: 3Sep2007 15:18:02 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48039; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:18:04 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 72.253.127.9; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2876; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:16:38 accept 192.168.99.1 >eth5 rule: 111; rule_uid: {AAAAAAAA-9999-8888-6F8CB5EB44F2}; service_id: CAP; src: 192.168.11.200; dst: 192.168.99.10; proto: tcp; product: VPN-1 & FireWall-1; service: 1026; s_port: 1640; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:18:07 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 47932; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:18:08 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48097; Sep 3 15:16:42 192.168.99.1 Checkpoint: 3Sep2007 15:16:41 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 24.92.226.9; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 40777; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:18:10 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 47993; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:18:11 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 47991; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:16:47 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1131; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:16:47 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 68.87.73.245; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 33100; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:18:15 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48061; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:16:47 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1132; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:16:48 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1133; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:16:48 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1134; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:16:48 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1135; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:16:48 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1136; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:16:49 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service:

80; s_port: 1137; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:16:49 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.229.56; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1139; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:16:49 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1140; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:16:49 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1141; Sep 3 15:16:48 192.168.99.1 Checkpoint: 3Sep2007 15:16:49 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41211; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:16:50 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1142; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:16:50 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1143; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:16:50 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1144; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:16:51 drop 192.168.99.1 >eth5 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.0.180; dst: 255.255.255.255; proto: udp; product: VPN-1 & FireWall-1; service: 67; s_port: 68; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:18:19 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41211; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:18:19 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48114; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:16:53 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1145; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:16:54 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1146; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:16:54 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1147; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:16:54 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1148; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:18:23 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 47909; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:16:57 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 68.87.73.244; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32960; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:16:57 accept 192.168.99.1 >eth8 rule: 122; rule_uid: {11111111-2222-3333-88DB-BA1479422786}; rule_name: Wireless; service_id: http; src: 192.168.99.23; dst: 153.2.228.50; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 1149; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:18:27 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-

A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48051; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:18:29 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbdatagram; src: 192.168.11.37; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138; Sep 3 15:17:00 192.168.99.1 Checkpoint: 3Sep2007 15:17:00 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 202.188.0.132; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32822; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:17:01 accept 192.168.99.1 >eth5 rule: 112; rule_uid: {11111111-2222-3333-97BB-2362F0B7F576}; src: 192.168.11.119; dst: 192.168.99.10; proto: udp; product: VPN-1 & FireWall-1; service: 389; s_port: 4919; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:17:01 accept 192.168.99.1 >eth5 rule: 112; rule_uid: {11111111-2222-3333-97BB-2362F0B7F576}; service_id: Kerberos_v5_UDP; src: 192.168.11.119; dst: 192.168.99.10; proto: udp; product: VPN-1 & FireWall-1; service: 88; s_port: 4920; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:18:30 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 47939; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:18:30 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48017; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:17:05 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 66.75.164.90; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 60893; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:18:33 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbdatagram; src: 192.168.11.202; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 138; s_port: 138; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:17:07 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; dst: 255.255.255.255; proto: udp; product: VPN-1 & FireWall-1; service: 67; s_port: 68; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:17:08 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 66.232.146.192; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 55675; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:17:08 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 200.33.146.233; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32777; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:17:08 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 200.33.146.169; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32777; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:18:36 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48046; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:17:11 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41212; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:17:11 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41213; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:17:11 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41214; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:17:11 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240;

dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41215; Sep 3 15:17:10 192.168.99.1 Checkpoint: 3Sep2007 15:17:11 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41216; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:17:11 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41217; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:17:11 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41218; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:18:39 accept 192.168.11.7 >eth8 rule: 116; rule_uid: {11111111-2222-3333-8836-09283F665349}; service_id: nbname; src: 192.168.11.34; dst: 192.168.11.255; proto: udp; product: VPN-1 & FireWall-1; service: 137; s_port: 137; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:18:40 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41212; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:18:40 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41213; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:18:40 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41214; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:18:40 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41215; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:18:40 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41216; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:18:40 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41217; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:18:41 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41218; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:17:13 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 200.23.242.209; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 55850; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:18:43 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48043; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:18:43 drop 192.168.11.7 >eth8 rule: 113; rule_uid: {AAAAAAAA-9999-8888-FFCF33A92D27}; service_id: http; src: 192.168.11.34; dst: 65.55.200.189; proto: tcp; product: VPN-1 & FireWall-1; service: 80; s_port: 2879; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:17:17 accept 192.168.99.1 >eth2 rule: 33; rule_uid: {AAAAAAAA-9999-8888-F33256AF77FB}; service_id: lotus; src: 192.168.13.103; dst: 192.168.99.13; proto: tcp; product: VPN-1 & FireWall-1; service: 1352; s_port: 1684; Sep 3 15:17:18 192.168.99.1 Checkpoint: 3Sep2007 15:17:17 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41219; Sep 3 15:17:26 192.168.99.1 Checkpoint: 3Sep2007 15:18:46 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum:

5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48084; Sep 3 15:17:26 192.168.99.1 Checkpoint: 3Sep2007 15:18:47 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41219; Sep 3 15:17:26 192.168.99.1 Checkpoint: 3Sep2007 15:17:19 accept 192.168.99.1 >eth8 rule: 40; rule_uid: {33333333-2222-1111-C048F9B6D5DA}; service_id: smtp; src: 192.168.99.185; dst: 192.168.13.18; proto: tcp; product: VPN-1 & FireWall-1; service: 25; s_port: 51744; Sep 3 15:17:26 192.168.99.1 Checkpoint: 3Sep2007 15:17:20 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 68.237.161.36; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32769; Sep 3 15:17:26 192.168.99.1 Checkpoint: 3Sep2007 15:17:20 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41220; Sep 3 15:17:26 192.168.99.1 Checkpoint: 3Sep2007 15:17:21 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41221; Sep 3 15:17:26 192.168.99.1 Checkpoint: 3Sep2007 15:17:21 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41222; Sep 3 15:17:27 192.168.99.1 Checkpoint: 3Sep2007 15:18:50 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41220; Sep 3 15:17:27 192.168.99.1 Checkpoint: 3Sep2007 15:18:50 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41221; Sep 3 15:17:27 192.168.99.1 Checkpoint: 3Sep2007 15:18:50 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41222; Sep 3 15:17:27 192.168.99.1 Checkpoint: 3Sep2007 15:17:23 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 148.160.29.6; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 33120; Sep 3 15:17:27 192.168.99.1 Checkpoint: 3Sep2007 15:17:24 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 194.204.159.8; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 32881; Sep 3 15:17:27 192.168.99.1 Checkpoint: 3Sep2007 15:17:24 accept 192.168.99.1 >eth2 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.13.3; dst: 192.168.99.10; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:17:27 192.168.99.1 Checkpoint: 3Sep2007 15:17:24 drop 192.168.99.1 >eth8 rule: 134; rule_uid: {11111111-2222-3333-BD17-711F536C7C33}; src: 192.168.99.185; dst: 192.149.252.44; proto: tcp; product: VPN-1 & FireWall-1; service: 43; s_port: 34350; Sep 3 15:17:27 192.168.99.1 Checkpoint: 3Sep2007 15:18:52 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48117; Sep 3 15:17:27 192.168.99.1 Checkpoint: 3Sep2007 15:18:55 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48023; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:18:56 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48126; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:18:56 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218;

dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48144; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:18:56 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48132; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:17:28 accept 192.168.99.1 >eth2 rule: 9; rule_uid: {11111111-2222-3333-8A67-F54CED606693}; service_id: domain-udp; src: 216.230.128.228; dst: 192.168.99.184; proto: udp; product: VPN-1 & FireWall-1; service: 53; s_port: 7186; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:18:57 accept 192.168.11.7 >eth2 rule: 99; rule_uid: {11111111-2222-3333-A397-FB37E6816BE5}; rule_name: NAT; service_id: http; src: 64.29.79.218; dst: 64.129.8.241; proto: tcp; xlatedst: 192.168.123.250; NAT_rulenum: 5; NAT_addtnl_rulenum: 0; product: VPN-1 & FireWall-1; service: 80; s_port: 48005; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:17:31 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41223; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:17:31 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41224; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:17:31 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41225; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:17:31 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41226; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:17:31 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41227; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:17:31 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41228; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:17:31 accept 192.168.99.1 >eth5 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41229; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:17:32 accept 192.168.99.1 >eth2 rule: 27; rule_uid: {33333333-2222-1111-A2B0-72699238CD27}; rule_name: Change after replacement; service_id: ntp-udp; src: 192.168.13.3; dst: 192.168.200.2; proto: udp; product: VPN-1 & FireWall-1; service: 123; s_port: 123; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:19:01 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41223; Sep 3 15:17:32 192.168.99.1 Checkpoint: 3Sep2007 15:19:01 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41224; Sep 3 15:17:52 192.168.99.1 Checkpoint: 3Sep2007 15:19:01 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41225; Sep 3 15:17:52 192.168.99.1 Checkpoint: 3Sep2007 15:19:01 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41226; Sep 3 15:17:52 192.168.99.1 Checkpoint: 3Sep2007 15:19:01 accept 192.168.11.7 >eth3 rule: 92; rule_uid: {11111111-2222-3333-2D9FEAB89E67}; rule_name: consultants API; service_id: consultants_API; src: 192.168.123.240; dst: 192.168.0.254; proto: tcp; product: VPN-1 & FireWall-1; service: 8000; s_port: 41227;

Log Samples from iptables

Martian log enabled:

UDP warning (netfilter module):

TCP shrunk window (netfilter module):

Microsoft ISA Server

Here is a sample of the firewall log from Microsoft ISA Server 2004 (in W3c extended format). Note that when the W3C extended log format is used, the times stamped on events are in Coordinated Universal Time (UTC) otherwise known as Greenwich Mean Time. So adjustments would have to be made during analysis for the particular time zone you are in.

Here is a sample of the web proxy log from ISA Server 2004. It is in W3C extended format.

Here are log samples from ISA Server 2000

IP Packet Filter log in W3C Extended format

2006-11-16 00:04:45 10.45.1.1 10.45.2.4 Udp 1675 137 - BLOCKED 10.45.1.1 23 44 44 4e yu bf 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8b 44 89 44 3a 82 37 2006-11-16 00:04:46 10.45.1.1 10.45.2.4 Udp 1675 137 - BLOCKED 10.45.1.1 23 44 44 4e yu c1 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8b 44 89 44 3a 82 35 2006-11-16 00:04:48 10.45.1.1 10.45.2.4 Udp 1675 137 - BLOCKED 10.45.1.1 23 44 44 4e yu c2 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8b 44 89 44 3a 82 33 2006-11-16 00:04:49 10.45.1.1 10.45.2.4 Udp 1675 137 - BLOCKED 10.45.1.1 23 44 44 4e yu ce 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8b 44 89 44 3a 82 31 2006-11-16 00:04:51 10.45.1.1 10.45.2.4 Udp 1675 137 - BLOCKED 10.45.1.1 23 44 44 4e yu cf 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8b 44 89 44 3a 82 2f 2006-11-16 00:08:51 10.45.1.1 10.45.2.4 Udp 1676 137 - BLOCKED 10.45.1.1 23 44 44 4e e6 61 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 4g 44 89 44 3a 82 26 2006-11-16 00:08:52 10.45.1.1 10.45.2.4 Udp 1676 137 - BLOCKED 10.45.1.1 23 44 44 4e e7 97 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 4g 44 89 44 3a 82 24 2006-11-16 00:08:54 10.45.1.1 10.45.2.4 Udp 1676 137 - BLOCKED 10.45.1.1 23 44 44 4e e8 4f 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 4g 44 89 44 3a 82 22 2006-11-16 00:08:55 10.45.1.1 10.45.2.4 Udp 1676 137 - BLOCKED 10.45.1.1 23 44 44 4e e9 d1 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 4g 44 89 44 3a 82 20 2006-11-16 00:08:57 10.45.1.1 10.45.2.4 Udp 1676 137 - BLOCKED 10.45.1.1 23 44 44 4e eb 4c 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 4g 44 89 44 3a 82 1e 2006-11-16 00:12:27 41.56.41.15 10.45.1.1 Tcp 80 24820 SYN ACK BLOCKED 10.45.1.1 23 44 44 30 bd eb 40 44 74 06 51 ac 0c 78 29 0f c0 a8 01 01 44 50 60 f4 ec f3 fc 84 h9 7d 10 a3 70 12 18 44 62 51 44 44 02 04 05 64 04 02 01 01 2006-11-16 00:12:28 41.56.41.15 10.45.1.1 Tcp 80 24820 SYN ACK BLOCKED 10.45.1.1 23 44 44 30 uj 0e 40 44 74 06 20 89 0c 78 29 0f c0 a8 01 01 44 50 60 f4 ec f3 fc 84 h9 7d 10 a3 70 12 18 44 62 51 44 44 02 04 05 64 04 02 01 01 2006-11-16 00:12:31 41.56.41.15 10.45.1.1 Tcp 80 24820 SYN ACK BLOCKED 10.45.1.1 23 44 44 30 11 61 40 44 74 06 fe 36 0c 78 29 0f c0 a8 01 01 44 50 60 f4 ec f3 fc 84 h9 7d 10 a3 70 12 18 44 62 51 44 44 02 04 05 64 04 02 01 01 2006-11-16 00:12:37 41.56.41.15 10.45.1.1 Tcp 80 24820 SYN ACK BLOCKED 10.45.1.1 23 44 44 30 57 15 40 44 74 06 b8 82 0c 78 29 0f c0 a8 01 01 44 50 60 f4 ec f3 fc 84 h9 7d 10 a3 70 12 18 44 62 51 44 44 02 04 05 64 04 02 01 01 2006-11-16 00:12:49 41.56.41.15 10.45.1.1 Tcp 80 24820 SYN ACK BLOCKED 10.45.1.1 23 44 44 30 b5 69 40 44 74 06 5a 2e 0c 78 29 0f c0 a8 01 01 44 50 60 f4 ec f3 fc 84 h9 7d 10 a3 70 12 18 44 62 51 44 44 02 04 05 64 04 02 01 01 2006-11-16 00:13:12 41.56.41.15 10.45.1.1 Tcp 80 24820 SYN ACK BLOCKED 10.45.1.1 23 44 44 30 58 ea 40 44 74 06 h9 yu 0c 78 29 0f c0 a8 01 01 44 50 60 f4 ec f3 fc 84 h9 7d 10 a3 70 12 18 44 62 51 44 44 02 04 05 64 04 02 01 01 2006-11-16 00:13:21 41.56.41.15 10.45.1.1 Tcp 80 24820 RST ACK BLOCKED 10.45.1.1 23 44 44 28 0f ca 40 44 74 06 ff d5 0c 78 29 0f c0 a8 01 01 44 50 60 f4 ec f3 fc 85 h9 7d 10 a3 50 14 44 44 a6 c1 44 00 2006-11-16 01:08:33 10.45.1.1 10.45.2.4 Udp 1677 137 - BLOCKED 10.45.1.1 23 44 44 4e 5c 5c 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8d 44 89 44 3a 81 9a 2006-11-16 01:08:34 10.45.1.1 10.45.2.4 Udp 1677 137 - BLOCKED 10.45.1.1 23 44 44 4e 5c 7e 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8d 44 89 44 3a 81 98 2006-11-16 01:08:36 10.45.1.1 10.45.2.4 Udp 1677 137 - BLOCKED 10.45.1.1 23 44 44 4e 5c f7 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8d 44 89 44 3a 81 96 2006-11-16 01:08:37 10.45.1.1 10.45.2.4 Udp 1677 137 - BLOCKED 10.45.1.1 23 44 44 4e 5d 75 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8d 44 89 44

3a 81 94 2006-11-16 01:08:39 10.45.1.1 10.45.2.4 Udp 1677 137 - BLOCKED 10.45.1.1 23 44 44 4e 5d bc 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8d 44 89 44 3a 81 92 2006-11-16 01:12:06 10.45.1.1 10.45.2.4 Udp 1678 137 - BLOCKED 10.45.1.1 23 44 44 4e 8f bc 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8e 44 89 44 3a 81 87 2006-11-16 01:12:08 10.45.1.1 10.45.2.4 Udp 1678 137 - BLOCKED 10.45.1.1 23 44 44 4e 90 96 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8e 44 89 44 3a 81 85 2006-11-16 01:12:09 10.45.1.1 10.45.2.4 Udp 1678 137 - BLOCKED 10.45.1.1 23 44 44 4e 91 bd 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8e 44 89 44 3a 81 83 2006-11-16 01:12:11 10.45.1.1 10.45.2.4 Udp 1678 137 - BLOCKED 10.45.1.1 23 44 44 4e 91 e0 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8e 44 89 44 3a 81 81 2006-11-16 01:12:12 10.45.1.1 10.45.2.4 Udp 1678 137 - BLOCKED 10.45.1.1 23 44 44 4e 92 11 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8e 44 89 44 3a 81 7f 2006-11-16 02:12:43 10.45.1.1 10.45.2.4 Udp 1679 137 - BLOCKED 10.45.1.1 23 44 44 4e 63 b5 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8f 44 89 44 3a 80 f6 2006-11-16 02:12:45 10.45.1.1 10.45.2.4 Udp 1679 137 - BLOCKED 10.45.1.1 23 44 44 4e 63 e0 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8f 44 89 44 3a 80 f4 2006-11-16 02:12:46 10.45.1.1 10.45.2.4 Udp 1679 137 - BLOCKED 10.45.1.1 23 44 44 4e 64 17 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8f 44 89 44 3a 80 f2 2006-11-16 02:12:48 10.45.1.1 10.45.2.4 Udp 1679 137 - BLOCKED 10.45.1.1 23 44 44 4e 64 5d 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8f 44 89 44 3a 80 f0 2006-11-16 02:12:49 10.45.1.1 10.45.2.4 Udp 1679 137 - BLOCKED 10.45.1.1 23 44 44 4e 64 73 44 44 80 11 44 44 c0 a8 01 01 c0 a8 02 04 06 8f 44 89 44 3a 80 ee

Here is the ISA Server 2000 Firewall Log in ISA Server format

Here is a sample of the ISA Server 2000 web proxy log in W3C Extended format

```
#Software: Microsoft(R) Internet Security and Acceleration Server 2000
#Version: 1.0
#Date: 2006-11-16 00:00:01
#Fields: c-ip cs-username     c-agent sc-authenticated        date    time    s-svcname       s-compu
10.54.80.151  anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.80.151  anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.29.65   ACME\clmantock  Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.43
10.54.29.65   ACME\clmantock  Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.43
10.54.80.151  ACME\eflynn     Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.20.97   anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Win32)       N       2006-11-16
10.54.20.97   anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Win32)       N       2006-11-16
10.54.20.97   ACME\capadonna  Mozilla/4.0 (compatible; MSIE 6.0; Win32)       Y       2006-11-16
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.70.45   anonymous       Acrobat Messages Updater        N       2006-11-16      00:00:09
10.54.80.133  ACME\rgordon    Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.80.133  anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.80.133  anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.70.99   anonymous       Acrobat Messages Updater        N       2006-11-16      00:00:12
10.54.35.2    anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
```

```
10.54.35.2    anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.35.2    anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.35.2    anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.30.132  ACME\rross      Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; .NET CLR 1.1.4322)
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.35.2    anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.35.2    anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.35.2    anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.35.2    anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.35.2    anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.35.2    anonymous       Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      N       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
10.54.35.2    ACME\hizzo      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)      Y       2006-11
-     -       Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) Active Cache Request N       2006-11
-     -       Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) Active Cache Request N       2006-11
-     -       Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) Active Cache Request N       2006-11
-     -       Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) Active Cache Request N       2006-11
-     -       Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) Active Cache Request N       2006-11
-     -       Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) Active Cache Request N       2006-11
-     -       Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) Active Cache Request N       2006-11
-     -       Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) Active Cache Request N       2006-11
-     -       Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) Active Cache Request N       2006-11
-     -       Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) Active Cache Request N       2006-11
```

A description of the fields in the ISA Server 2000 version log files can be found at this site.

A description of the fields in the ISA Server 2004 log files can be found **'at this site.http://msdn2.microsoft.com/en-us/library/aa503237.aspx>'_**

Other general information about ISA Server and ISA Server logs can be found at the following links:

Official Microsoft site for ISA Server 2000

Official Microsoft site for ISA Server 2004

Official Microsoft site for ISA Server 2006

Microsoft ISA Server Firewall Resource Site: Articles and Tutorials

‘ ISA Server 2000 Alerts, Reports and Logs FAQ <http://www.microsoft.com/technet/isa/2000/maintain/isafaqra.mspx>‘_

Configuring ISA Server 2000 log files

How to Configure Logging in ISA Server 2000

ISA Server 2000 Monitoring Concepts: Logging

ISA Server 2000 Packet Filtering

About the ISA Server 2000 Firewall

ISA Server 2004 best practices: Logging

Description of the time format used in ISA Server 2004 logs

ISA Server 2004 Monitoring Concepts:Logs

ISA Server 2004 Log Code Values

Understanding ISA Server 2004 Monitoring

ISA Server 2006 Logging Fields and Values

Log Samples from the Netscreen Firewall

Traffic denied:

```
Jun  2 14:55:46 fire00 fire00: NetScreen device_id=fire00  [Root]system-notification-00257(traffic):
Jun  2 14:53:31 fire00 aka1: NetScreen device_id=aka1  [Root]system-notification-00257(traffic): sta
Jun  2 14:53:31 fire00 aka1: NetScreen device_id=aka1  [Root]system-notification-00257(traffic): sta
Mar 16 15:27:56 172.16.10.42 ns5gt: NetScreen device_id=ns5gt  [No Name]system-notification-00257(tra
```

Alert messages:

```
Jun  1 22:01:35 [xx] ns5gt: NetScreen device_id=ns5gt  [Root]system-alert-00016: Port scan! From 1.2
Jun  1 22:01:57 [xx] ns5gt: NetScreen device_id=ns5gt  [Root]system-alert-00016: Port scan! From 1.2
Jun  1 22:02:10 [xx] ns5gt: NetScreen device_id=ns5gt  [Root]system-alert-00016: Port scan! From 1.2
```

Critical messages:

Admin login:

```
Jun  1 22:02:12 [xx] ns5gt: NetScreen device_id=ns5gt  [Root]system-notification-00002: Admin user "h
```

Log samples from PF

Various versions of PF currently run on OpenBSD, FreeBSD, NetBSD, DragonflyBSD, and Mac OS X 10.6. For details on how to configure it, check the pf FAQ

```
Mar 30 15:55:20 enigma pf: Mar 30 15:53:25.793256 rule 2/(match) pass in on xl0: 205.174.165.231.5042
Mar 30 15:55:20 enigma pf: Mar 30 15:53:25.815208 rule 2/(match) pass in on xl0: 205.174.165.231.5042
Mar 30 15:55:20 enigma pf: Mar 30 15:53:25.844763 rule 2/(match) pass in on xl0: 205.174.165.231.5042
Mar 30 15:55:20 enigma pf: Mar 30 15:53:25.867973 rule 2/(match) pass in on xl0: 205.174.165.231.5042
Mar 30 15:55:20 enigma pf: Mar 30 15:53:25.892592 rule 2/(match) pass in on xl0: 205.174.165.231.5042
Mar 30 15:55:20 enigma pf: Mar 30 15:53:25.916465 rule 2/(match) pass in on xl0: 205.174.165.231.5042
Mar 30 15:55:20 enigma pf: Mar 30 15:53:25.945039 rule 2/(match) pass in on xl0: 205.174.165.231.5042
Mar 30 15:55:20 enigma pf: Mar 30 15:53:25.966970 rule 2/(match) pass in on xl0: 205.174.165.231.5042
Mar 30 15:55:20 enigma pf: Mar 30 15:53:25.968177 rule 2/(match) pass in on xl0: 205.174.165.231.5042
Mar 30 15:55:20 enigma pf: Mar 30 15:54:39.257554 rule 3/(match) pass out on xl0: 192.168.2.10.22 > 2
Mar 30 15:55:20 enigma pf: Mar 30 15:55:14.265470 rule 3/(match) pass out on xl0: 192.168.2.10.1514 >
Mar 30 15:55:20 enigma pf: Mar 30 15:55:14.267876 rule 3/(match) pass out on xl0: 192.168.2.10.1514 >
Mar 30 15:55:20 enigma pf: Mar 30 15:55:14.270532 rule 3/(match) pass out on xl0: 192.168.2.10.1514 >
Mar 30 15:55:20 enigma pf: Mar 30 15:55:14.273141 rule 3/(match) pass out on xl0: 192.168.2.10.1514 >
Mar 30 15:55:20 enigma pf: Mar 30 15:55:14.275813 rule 3/(match) pass out on xl0: 192.168.2.10.1514 >
Mar 30 15:55:20 enigma pf: Mar 30 15:55:14.278266 rule 3/(match) pass out on xl0: 192.168.2.10.1514 >
Mar 30 15:55:20 enigma pf: Mar 30 15:55:14.281040 rule 3/(match) pass out on xl0: 192.168.2.10.1514 >
Mar 30 15:55:20 enigma pf: Mar 30 15:55:14.283846 rule 3/(match) pass out on xl0: 192.168.2.10.1514 >
Mar 30 15:55:20 enigma pf: Mar 30 15:55:14.286602 rule 3/(match) pass out on xl0: 192.168.2.10.1514 >
Mar 30 15:55:20 enigma pf: Mar 30 15:55:14.289160 rule 3/(match) pass out on xl0: 192.168.2.10.1514 >
Mar 30 15:55:19 enigma pf: Mar 30 15:48:02.810188 rule 2/(match) pass in on lo0: 127.0.0.1 > 127.0.0.
Mar 30 15:55:19 enigma pf: Mar 30 15:48:03.688233 rule 3/(match) pass out on xl0: 192.168.2.10 > 192.
Mar 30 15:55:19 enigma pf: Mar 30 15:48:03.820068 rule 3/(match) pass out on lo0: 127.0.0.1 > 127.0.0
Mar 30 15:55:19 enigma pf: Mar 30 15:48:03.820087 rule 2/(match) pass in on lo0: 127.0.0.1 > 127.0.0.
Mar 30 15:55:19 enigma pf: Mar 30 15:48:03.820115 rule 3/(match) pass out on lo0: 127.0.0.1 > 127.0.0
Mar 30 15:55:19 enigma pf: Mar 30 15:48:03.820129 rule 2/(match) pass in on lo0: 127.0.0.1 > 127.0.0.
Mar 30 15:55:19 enigma pf: Mar 30 15:48:04.830069 rule 3/(match) pass out on lo0: 127.0.0.1 > 127.0.0
Mar 30 15:55:19 enigma pf: Mar 30 15:48:04.830088 rule 2/(match) pass in on lo0: 127.0.0.1 > 127.0.0.
Mar 30 15:55:19 enigma pf: Mar 30 15:48:04.830118 rule 3/(match) pass out on lo0: 127.0.0.1 > 127.0.0
Mar 30 15:55:19 enigma pf: Mar 30 15:48:04.830132 rule 2/(match) pass in on lo0: 127.0.0.1 > 127.0.0.
```

Log Samples from SonicWall

Log explained: http://www.sonicwall.com/downloads/SonicOS_Log_Event_Reference_Guide.pdf

General logs:

Dropped events:

Apr 1 10:45:16 10.1.5.1 id=firewall sn=00301E0526B1 time="2004-04-01 10:39:35" fw=67.32.44.2 pri=5 c=64 m=36 msg="TCP connection dropped" n=2686 src=67.101.200 .27:4507:WAN dst=67.32.44.2:445:LAN proto=tcp

Samples for the Windows firewall

By default the logs are stored at <b>C:Windowspfirewall.log.

Fields:

Firewall drop:

```
2006-09-19 10:48:12 DROP UDP 172.20.73.241 239.255.255.250 2250 1900 250 - - - - - - - - RECEIVE
2006-09-20 10:38:21 DROP TCP 192.168.72.196 10.20.72.12 445 2459 48 SA 4175551841 892874455 17520 - -
```

Firewall Accept:

```
2006-09-19 03:04:29 OPEN TCP 192.168.72.12 10.20.72.204 3599 445 - - - - - - - - - -
2006-09-19 03:04:29 OPEN TCP 192.168.72.12 10.20.72.204 3600 139 - - - - - - - - - -
```

Large sample:

Sample 2:

WIPFW

Here is a log sample from the WIPFW firewall for Windows. More information about WIPFW can be found at http://wipfw.sourceforge.net. If you're using Windows, I can't recommend WIPFW highly enough. It is Open Source and is the most highly configurable firewall product I've found for Windows to date. (Understand WIPFW is a straight network firewall; it does no application access control or anything along those lines. If that's what you need, you'll need to use something else like [[Zone_Alarm|Zone Alarm]].)

WIPFW puts these logs in your C:Windowssecuritylogs directory. The log format is fairly simple. The first number is the log entry, followed by the date and the time. After "ipfw:" is the firewall rule number (1000 in the above example), followed by the action and the protocol. The rest is self-explanatory.

Zone Alarm (free version) Log samples

Details about Zone Alarm and it's logging features (including text log field descriptions) can be found in the [http://download.zonelabs.com/bin/media/pdf/zaclient65_user_manual.pdf ZoneAlarm manual]

The logfile can be tab, comma, or semi-colon delimited (user can make the choice).

Logfile located (on Windows XP) in C:WINDOWSInternet Logs

Filename = ZALog.txt:

More log samples showing different kinds of entries:

Courier Log samples

Pop3 Login failed:

```
May 30 00:01:02 server2 courierpop3login: LOGIN FAILED, ip=[::ffff:193.68.217.36]
May 30 00:01:03 server2 courierpop3login: LOGIN FAILED, ip=[::ffff:193.68.217.36]
May 30 00:01:02 server2 courierpop3login: LOGIN FAILED, ip=[::ffff:193.68.217.36]

Dec 1 10:46:22 debian courierpop3login: LOGIN FAILED, ip=[::ffff:192.168.1.161]
```

```
Dec 1 10:46:30 debian courierpop3login: Connection, ip=[::ffff:192.168.1.161]
Dec 1 10:46:35 debian courierpop3login: LOGIN FAILED, ip=[::ffff:192.168.1.161]

Nov 22 20:02:24 www courierpop3login: LOGIN FAILED, ip=[::ffff:192.168.0.188]
Nov 22 20:02:26 www courierpop3login: LOGIN FAILED, ip=[::ffff:5.4.234.42]
Nov 22 20:02:26 www courierpop3login: LOGOUT, ip=[::ffff:5.4.234.42]
Nov 22 20:02:26 www courierpop3login: Connection, ip=[::ffff:5.4.234.42]
Nov 22 20:02:30 www courierpop3login: LOGIN FAILED, ip=[::ffff:62.10.125.238]
Nov 22 20:02:34 www courierpop3login: LOGIN FAILED, ip=[::ffff:5.4.234.42]
Nov 22 20:02:34 www courierpop3login: LOGOUT, ip=[::ffff:5.4.234.42]
```

Pop3d-ssl Login failed:

```
Jan 3 02:07:37 web pop3d-ssl: Connection, ip=[::ffff:192.168.0.200]
Jan 3 02:07:44 web pop3d-ssl: LOGIN FAILED, ip=[::ffff:192.168.0.200]
```

Imapd Login failed:

```
Sep 21 00:40:57 server01 imaplogin: LOGIN FAILED, ip=[::ffff:127.0.0.1]
Sep 21 00:41:17 server01 imaplogin: LOGIN FAILED, ip=[::ffff:127.0.0.1]
Sep 21 00:42:21 server01 imaplogin: LOGIN FAILED, ip=[::ffff:127.0.0.1]
Sep 21 00:42:21 server01 imaplogin: DISCONNECTED, ip=[::ffff:127.0.0.1], time=5
Sep 21 00:42:28 server01 imaplogin: LOGIN FAILED, ip=[::ffff:127.0.0.1]
Sep 21 00:44:23 server01 imaplogin: DISCONNECTED, ip=[::ffff:127.0.0.1], time=0
Sep 21 00:48:58 server01 courierpop3login: LOGIN FAILED, ip=[::ffff:88.73.124.13]
Sep 21 00:49:42 server01 imaplogin: LOGIN FAILED, ip=[::ffff:127.0.0.1]
Sep 21 00:51:50 server01 courierpop3login: LOGIN FAILED, ip=[::ffff:88.73.124.13]
Sep 21 00:53:42 server01 courierpop3login: LOGIN FAILED, ip=[::ffff:88.73.124.13]
```

Valid logins:

```
Jun 1 00:12:06 server1 courierpop3login: LOGIN, user=web10_mauricio, ip=[::ffff:192.168.0.100]
Jun 1 00:12:06 server1 courierpop3login: LOGOUT, user=web10_mauricio, ip=[::ffff:192.168.0.100], top=
Jun 1 00:21:40 server1 courierpop3login: Connection, ip=[::ffff:192.168.0.100]
Jun 1 00:21:40 server1 courierpop3login: LOGIN, user=web10_mauricio, ip=[::ffff:192.168.0.100]
Jun 1 00:21:40 server1 courierpop3login: LOGOUT, user=web10_mauricio, ip=[::ffff:192.168.0.100], top=
Jun 1 00:30:15 server1 courierpop3login: Connection, ip=[::ffff:192.168.0.100]
Jun 1 00:30:15 server1 courierpop3login: LOGIN, user=web10_mauricio, ip=[::ffff:192.168.0.100]
Jun 1 00:30:15 server1 courierpop3login: LOGOUT, user=web10_mauricio, ip=[::ffff:192.168.0.100], top=
Jun 1 00:31:40 server1 courierpop3login: Connection, ip=[::ffff:192.168.0.100]
Jun 1 00:31:40 server1 courierpop3login: LOGIN, user=web10_mauricio, ip=[::ffff:192.168.0.100]
Jun 1 00:31:40 server1 courierpop3login: LOGOUT, user=web10_mauricio, ip=[::ffff:192.168.0.100], top=
```

Dovecot log samples

IMAP:

Login:

Error time change:

Logout/Connection close:

Error auth:

Attacks:

POP3:

Login:

Logout/Connection close:

Error time change:

Error auth:

AUTH:

Error time change:

Errors:

OTHERS:

Exchange Log Samples

Here are two different formats of the Exchange 2000 SMTP logs.

W3C Extended format:

NCSA format:

```
205.188.158.121 - OutboundConnectionResponse [11/Oct/2006:13:16:39 -0600] "- -?220-rly-yi06.mx.aol.co
205.188.158.121 - OutboundConnectionCommand [11/Oct/2006:13:16:39 -0600] "EHLO -?mee-pdc.meelift.com
205.188.158.121 - OutboundConnectionResponse [11/Oct/2006:13:16:39 -0600] "- -?250-rly-yi06.mx.aol.co
61.47.65.115 - 207.250.64.66 [11/Oct/2006:13:16:40 -0600] "HELO -?+207.250.64.66 SMTP" 250 46
61.47.65.115 - 207.250.64.66 [11/Oct/2006:13:16:41 -0600] "MAIL -?+FROM:+<Keith@boardermail.com> SMTP
61.47.65.115 - 207.250.64.66 [11/Oct/2006:13:16:41 -0600] "RCPT -?+TO:+<s-r_kke@meelift.com> SMTP" 25
61.47.65.115 - 207.250.64.66 [11/Oct/2006:13:16:42 -0600] "RCPT -?+TO:+<s-r_mke@meelift.com> SMTP" 25
83.44.189.146 - 1stallied.com [11/Oct/2006:13:16:43 -0600] "HELO -?+1stallied.com SMTP" 250 47
61.47.65.115 - 207.250.64.66 [11/Oct/2006:13:16:43 -0600] "RCPT -?+TO:+<dbveto@meelift.com> SMTP" 250
```

```
83.44.189.146 - 1stallied.com [11/Oct/2006:13:16:43 -0600] "MAIL -?+FROM:<penwine@1stallied.com> SMTP
83.44.189.146 - 1stallied.com [11/Oct/2006:13:16:43 -0600] "RCPT -?+TO:<rcutsforth@meelift.com> SMTP"
61.47.65.115 - 207.250.64.66 [11/Oct/2006:13:16:44 -0600] "RCPT -?+TO:+<pamb@meelift.com> SMTP" 250 2
61.47.65.115 - 207.250.64.66 [11/Oct/2006:13:16:44 -0600] "RCPT -?+TO:+<tom@meelift.com> SMTP" 250 28
83.44.189.146 - 1stallied.com [11/Oct/2006:13:16:45 -0600] "DATA -?+<000001c6ed61$33a7e690$97cfa8c0@e
83.44.189.146 - 1stallied.com [11/Oct/2006:13:16:45 -0600] "QUIT -?1stallied.com SMTP" 240 68
65.214.43.171 - - [11/Oct/2006:13:16:47 -0600] "xxxx -?+armin.techtarget.com SMTP" 500 32
61.47.65.115 - 207.250.64.66 [11/Oct/2006:13:16:47 -0600] "RCPT -?+TO:+<tkappers@meelift.com> SMTP" 2
65.214.43.171 - armin.techtarget.com [11/Oct/2006:13:16:48 -0600] "HELO -?+armin.techtarget.com SMTP"
65.214.43.171 - armin.techtarget.com [11/Oct/2006:13:16:49 -0600] "MAIL -?+FROM:<567507-dbveto=meelif
61.47.65.115 - 207.250.64.66 [11/Oct/2006:13:16:50 -0600] "DATA -?+<10100.marigold@cleat> SMTP" 250 1
61.47.65.115 - 207.250.64.66 [11/Oct/2006:13:16:50 -0600] "QUIT -?207.250.64.66 SMTP" 240 68
65.214.43.171 - armin.techtarget.com [11/Oct/2006:13:16:51 -0600] "RCPT -?+TO:<dbveto@meelift.com> SM
81.196.176.167 - - [11/Oct/2006:13:16:54 -0600] "xxxx -?+81-196-176-167.rdsnet.ro SMTP" 500 32
81.196.176.167 - 81-196-176-167.rdsnet.ro [11/Oct/2006:13:16:54 -0600] "HELO -?+81-196-176-167.rdsnet
81.196.176.167 - 81-196-176-167.rdsnet.ro [11/Oct/2006:13:16:55 -0600] "MAIL -?+FROM:<sshambeau@meeli
81.196.176.167 - 81-196-176-167.rdsnet.ro [11/Oct/2006:13:16:55 -0600] "RCPT -?+TO:<sshambeau@meelift
81.196.176.167 - 81-196-176-167.rdsnet.ro [11/Oct/2006:13:16:56 -0600] "DATA -?+<000901c6ed61$6e8f3f1
81.196.176.167 - 81-196-176-167.rdsnet.ro [11/Oct/2006:13:16:56 -0600] "QUIT -?81-196-176-167.rdsnet.
205.188.158.121 - OutboundConnectionCommand [11/Oct/2006:13:17:02 -0600] "MAIL -?FROM:<pbourque@meeli
205.188.158.121 - OutboundConnectionResponse [11/Oct/2006:13:17:02 -0600] "- -?250+OK SMTP" 0 6
205.188.158.121 - OutboundConnectionCommand [11/Oct/2006:13:17:02 -0600] "RCPT -?TO:<kbee923@aol.com>
205.188.158.121 - OutboundConnectionResponse [11/Oct/2006:13:17:02 -0600] "- -?250+OK SMTP" 0 6
205.188.158.121 - OutboundConnectionCommand [11/Oct/2006:13:17:02 -0600] "DATA - SMTP" 0 4
205.188.158.121 - OutboundConnectionResponse [11/Oct/2006:13:17:02 -0600] "- -?354+START+MAIL+INPUT,+
205.188.158.121 - OutboundConnectionResponse [11/Oct/2006:13:17:04 -0600] "- -?250+OK SMTP" 0 6
205.188.158.121 - OutboundConnectionCommand [11/Oct/2006:13:17:04 -0600] "QUIT - SMTP" 0 4
205.188.158.121 - OutboundConnectionResponse [11/Oct/2006:13:17:04 -0600] "- -?221+SERVICE+CLOSING+CH
217.169.41.109 - outbound.emediausa.com [11/Oct/2006:13:17:13 -0600] "HELO -?+outbound.emediausa.com
217.169.41.109 - outbound.emediausa.com [11/Oct/2006:13:17:17 -0600] "MAIL -?+FROM:<Subscriber.10804
217.169.41.109 - outbound.emediausa.com [11/Oct/2006:13:17:17 -0600] "RCPT -?+TO:<dbveto@meelift.com>
```

Log Samples from Exim

I've included the ossec bad responses:

*error 450 (ossec should probably ignore) – this particular line is blowback from spam delivery attempt elsewhere with one of our addresses spoofed as "From", and occurs many times in the log files

```
Received From: (mailserver) 192.168.1.21->/var/log/mail.log
Rule: 1002 fired (level 7) -> "Unknown problem somewhere in the system."
Portion of the log(s):

exim[14700]: 2006-11-21 15:01:33 1Glsgv-0002wv-00 SMTP error from remote mailer after RCPT TO:<xxxxxx
```

*error 550 (ossec should ignore after the first time) .. code-block:: console

> Received From: (mailserver) 192.168.1.21->/var/log/mail.log Rule: 1002 fired (level 7) -> "Unknown problem somewhere in the system." Portion of the log(s):
>
> exim[14706]: 2006-11-21 15:01:39 1Gmary-0002iA-00 ** xxxxxxxx@some-domain.com R=dnslookup T=remote_smtp: SMTP error from remote mailer after RCPT TO:<xxxxxxxx@some-domain.com>: host mx.some-domain.com [1.1.1.1]: 550 Mailbox unavailable <xxxxxxxxxxx@some-domain.com>

*frozen (probably okay to ignore) .. code-block:: console

> Received From: (mailserver) 192.168.1.21->/var/log/mail.log Rule: 1002 fired (level 7) -> "Unknown problem somewhere in the system." Portion of the log(s):

exim[15745]: 2006-11-21 15:17:10 1Gmc37-00045w-00 Frozen (delivery error message)

*local delivery error (unknown user most likely, probably okay to ignore) although parsing out the email address and IP could provide a trigger for an active response (e.g. a honeypot email address that triggers the sending IP address to be blocked for 24 hours) .. code-block:: console

Received From: (mailserver) 192.168.1.21->/var/log/mail.log Rule: 1002 fired (level 7) -> "Unknown problem somewhere in the system." Portion of the log(s):

exim[15740]: 2006-11-21 15:16:57 1Gmc36-00045o-00 ** xxxxxxxxxxx@some-domain.com R=local_user_cyrus T=local_delivery_cyrus: Child process of local_delivery_cyrus transport returned 65 (could mean error in input data) from command: /usr/cyrus/bin/deliver

*this error 450 should be a 550 – ossec could ignore (it's a temporary error message for a permanent error, but not much we can do about it) .. code-block:: console

Received From: (mailserver) 192.168.1.21->/var/log/mail.log Rule: 1002 fired (level 7) -> "Unknown problem somewhere in the system." Portion of the log(s):

exim[16042]: 2006-11-21 15:24:02 1Gm2od-0001ay-00 xxxxxxxxxxx@some-domain.com R=dnslookup T=remote_smtp defer (0): SMTP error from remote mailer after RCPT TO:<xxxxxxxxxxx@some-domain.com>: host mail.some-domain.com [66.93.22.101]: 450 <xxxxxxxxxxx@some-domain.com>: User unknown in local recipient table

*Connection refused; not much we can do about this error either .. code-block:: console

Received From: (mailserver) 192.168.1.21->/var/log/mail.log Rule: 1002 fired (level 7) -> "Unknown problem somewhere in the system." Portion of the log(s):

exim[14164]: 2006-11-21 14:55:07 1GlKR9-0003x0-00 xxxxxxx@some-domain.com R=dnslookup T=remote_smtp defer (111): Connection refused

*error 501 – most likely the recipient's DNS is misconfigured; but this is most likely blowback from spam, so it's not terribly important .. code-block:: console

Received From: (mailserver) 192.168.1.21->/var/log/mail.log Rule: 1002 fired (level 7) -> "Unknown problem somewhere in the system." Portion of the log(s):

exim[13428]: 2006-11-21 14:39:59 1GmbTK-0003UZ-00 ** xxxxxxxx@somedomain.com R=dnslookup T=remote_smtp: SMTP error from remote mailer after RCPT TO:<xxxxxxxx@somedomain.com>: host mail.somedomain.com [1.1.3.1]: 501 This system is not configured to relay mail (r) to <somedomain.com> for 2.2.1.5

Log Samples from imapd

Failed logins:

```
imapd[25015]: Login failed user=grasielle auth=grasielle host=imapd.lab.ossec.net [1.2.3.4]
imapd[25015]: Login failed user=grasielle auth=grasielle host=imapd.lab.ossec.net [1.2.3.4]
```

Log Samples for postfix

Postfix internal error:

postfix/bounce[21172]: fatal: lock file defer 4438F62ECB: Resource temporarily unavailable postfix/smtpd[21779]: warning: connect to private/policy: Resource temporarily unavailable postfix/smtp[30785]: warning: 75FEC31D36: defer service failure postfix/postfix-script: fatal: the Postfix mail system is not running

Email rejected (source blacklisted):

postfix/smtpd[10419]: NOQUEUE: reject: RCPT from unknown[200.71.50.65]: 554 Service unavailable; Client host [200.71.50.65] blocked using sbl-xbl.spamhaus.org; http://www.spamhaus.org/query/bl?ip=200.71.50.65; from=<kpxbeiu@superig.com.br> to=<cleresilva@lac.ossec.net> proto=SMTP helo=<Static-IP-cr200715065.cable.net.co>

postfix/smtpd[13496]: NOQUEUE: reject: RCPT from pool-71-121-135-165.sttlwa.dsl-w.verizon.net[71.121.135.165]: 554 Service unavailable; Client host [71.121.135.165] blocked using sbl-xbl.spamhaus.org; http://www.spamhaus.org/query/bl?ip=71.121.135.165; from=<vxznjomowm@directnet.com.br> to=<lala@lac.ossec.net> proto=SMTP helo=<pool-71-121-135-165.sttlwa.dsl-w.verizon.net>

Spam attempts:

postfix/smtpd[6741]: NOQUEUE: reject: RCPT from unknown[201.82.55.24]: 503 <nplxf-btk@fbi.com>: Sender address rejected: Improper use of SMTP command pipelining; from=<nplxfbtk@fbi.com> to=<x@x.br> proto=SMTP helo=<ran-2h991bqbujq>

postfix/smtpd[6741]: NOQUEUE: reject: RCPT from unknown[201.82.55.24]: 503 <nplxf-btk@fbi.com>: Sender address rejected: Improper use of SMTP command pipelining; from=<nplxfbtk@fbi.com> to=<x@xl.org.br> proto=SMTP helo=<ran-2h991bqbujq>

Insufficient storage:

helo=<217-133-56-239.b2b.tiscali.it> Jun 29 17:28:38 linuxserver postfix/smtpd[27712]: NOQUEUE: reject: MAIL from localhost[127.0.0.1]: 452 Insufficient system storage; proto=ESMTP helo=<localhost>

Some postfix errors:

Log Samples from Sendmail

Error code 553, rejected due to spam:

Connection rate limit exceeded (421 4.3.2):

Pre-greeting traffic (rejected):

Jul 20 16:21:24 mx0 sendmail[7818]: j6KKHo2d007818: rejecting commands from sv.e103gng.com [66.62.19.10] due to pre-greeting traffic

SMF-SAV Sendmail Milter decoder:

smf-sav[513]: [ID 987462 mail.notice] sender check failed: <xkyjywqvophshu@mypersonalemail.com>, 125.133.22.112, [125.133.22.112], [00:00:01] smf-sav[513]: [ID 407019 mail.info] sender check succeeded (cached): <asterisk-users-bounces@lists.digium.com>, 216.207.245.17, lists.digium.com smf-sav[513]: [ID 987894

mail.notice] sender check tempfailed: <31363****-org@targetedpages.com>, 69.8.190.101, smtp101.tramailer.info, [00:00:05]

Save mail panic:

Log Samples for VM-POP3d

Log Samples from vpopmail

Failed logins:

```
Sep 14 07:21:42 iron vpopmail[939]: vchkpw-pop3: password fail user1@xxxx.com:192.168.2.1
Sep 14 07:21:42 iron vpopmail[937]: vchkpw-pop3: password fail user2@xxxx.com:192.168.2.1
Sep 14 07:21:42 iron vpopmail[935]: vchkpw-pop3: password fail user3@xxxx.com:192.168.2.1
Jun 9 08:56:30 www vpopmail[65827]: vchkpw-smtp: password fail (pass: '<65825.1118321790@mail.xxx.cor
```

Invalid user:

```
vpopmail[2100]: vchkpw-pop3: vpopmail user not found abc@xxx.com:x.x.x.x
vpopmail[65851]: vchkpw-pop3: vpopmail user not found myuserid@:208.210.222.68
```

Full samples:

Brute Force Attack:

Log samples from vpopmail and qmailtoaster

In qmailtoaster vpopmail can be use for: pop3, pop3s, imap, imaps, smtp, submission and webmail. Therefore each record can include respectively: * vchkpw-pop3: * vchkpw-pop3s: * vchkpw-imap: * vchkpw-imaps: * vchkpw-smtp: * vchkpw-submission: * vchkpw-webmail:

Succesfull login:

Bad password:

or if no password given:

Invalid user:

Log Samples for VMware ESX

From /var/log/vmware/hostd.log:

From /var/log/secure (user logins, etc):

Web Scan sample 2

Example of web scan detected by ossec (looking for Wordpress, xmlrpc and awstats):

Web scan sample 4:

SSHD brute force:

Example of a SSHD brute force attack.

FTP Scan:

Example of FTP scan detected by monitoring MS FTP logs.

Multiple firewall denies on the Windows firewall:

Example of multiple firewall denies detected. .. code-block:: console

> Received From: (ossec64) 192.168.2.25->Windowspfirewall.log Rule: 4151 fired (level 10) -> "Multiple Firewall drop events from same source." Portion of the log(s):
>
> 2006-10-17 09:25:03 DROP UDP 192.168.2.190 192.168.2.255 137 137 78 - - - - - - - RECEIVE 2006-10-17 09:25:01 DROP UDP 192.168.2.190 192.168.2.255 138 138 229 - - - - - - - RECEIVE 2006-10-17 09:25:00 DROP UDP 192.168.2.190 192.168.2.255 137 137 96 - - - - - - - RECEIVE 2006-10-17 09:25:00 DROP UDP 192.168.2.190 192.168.2.255 137 137 96 - - - - - - - RECEIVE 2006-10-17 09:24:59 DROP UDP 192.168.2.190 192.168.2.255 137 137 96 - - - - - - - RECEIVE 2006-10-17 09:24:59 DROP UDP 192.168.2.190 192.168.2.255 137 137 96 - - - - - - - RECEIVE 2006-10-17 09:24:59 DROP UDP 192.168.2.190 192.168.2.255 137 137 96 - - - - - - - RECEIVE 2006-10-17 09:24:59 DROP UDP 192.168.2.190 192.168.2.255 137 137 96 - - - - - - - RECEIVE 2006-10-17 09:24:58 DROP UDP 192.168.2.190 192.168.2.255 137 137 96 - - - - - - - RECEIVE 2006-10-17 09:24:58 DROP UDP 192.168.2.190 192.168.2.255 137 137 96 - - - - - - - RECEIVE
>
> —END OF NOTIFICATION

Multiple spam attempts:

Example of spam attempts detected (postix log analysis)

postfix/smtpd[6741]: NOQUEUE: reject: RCPT from unknown[201.82.55.24]: 503 <nplxfbtk@fbi.com>: Sender address rejected: Improper use of SMTP command pipelining; from=<nplxfbtk@fbi.com> to=<x@x.br> proto=SMTP helo=<ran-2h991bqbujq> postfix/smtpd[6741]: NOQUEUE: reject: RCPT from unknown[201.82.55.24]: 503 <nplxfbtk@fbi.com>: Sender address rejected: Improper use of SMTP command pipelining; from=<nplxfbtk@fbi.com> to=<x@xl.org.br> proto=SMTP helo=<ran-2h991bqbujq> postfix/smtpd[6741]: NOQUEUE: reject: RCPT from unknown[201.82.55.24]: 503 <nplxfbtk@fbi.com>: Sender address rejected: Improper use of SMTP command pipelining; from=<nplxfbtk@fbi.com> to=<y@y.org.br> proto=SMTP helo=<ran-2h991bqbujq> postfix/smtpd[6741]: NOQUEUE: reject: RCPT from unknown[201.82.55.24]: 503 <nplxfbtk@fbi.com>: Sender address rejected: Improper use of SMTP command pipelining; from=<nplxfbtk@fbi.com> to=<z@l.org.br> proto=SMTP helo=<ran-2h991bqbujq> postfix/smtpd[6741]: NOQUEUE: reject: RCPT from unknown[201.82.55.24]: 503 <nplxfbtk@fbi.com>: Sender address rejected: Improper use of SMTP command pipelining; from=<nplxfbtk@fbi.com> to=<a@slala.org.br> proto=SMTP helo=<ran-2h991bqbujq> postfix/smtpd[6741]: NOQUEUE: reject: RCPT from unknown[201.82.55.24]: 503 <nplxfbtk@fbi.com>: Sender address rejected: Improper use of SMTP command pipelining; from=<nplxfbtk@fbi.com> to=<b@l.org.br> proto=SMTP helo=<ran-2h991bqbujq> postfix/smtpd[6741]: NOQUEUE: reject: RCPT from unknown[201.82.55.24]: 503 <nplxfbtk@fbi.com>: Sender address rejected: Improper use of SMTP command pipelining; from=<nplxfbtk@fbi.com> to=<c@y.org.br> proto=SMTP helo=<ran-2h991bqbujq>

SQL Injection attempt detected:

Example of an SQL injection detected by ossec:

Internal system possibly compromised with IrnBot:

http://www.offensivecomputing.net/?q=node/378

==Multiple WordPress (blog) comment spam attempts==

Attempts to submit spammer comments to the ossec blog:

E-mail scan (vpopmail):

File system full:

Not really an attack, but a serious issue if your web server is out of space.

Custom SQL injection against ossec.net:

Someone trying our web application to display the latest rules. Of course, it didn't work
 (but we return code 200 on all cases).

Application being installed:

An alert when an application is installed on Windows. Not always an attack, but may indicate a computer misuse.

Virtual machine being shut down:

By monitoring VMware ESX logs, you can get alerts when a virtual machine is stopped:

2.6 Glossary

HIDS First of all, Intrusion Detection is the process or techniques used to detect attacks on a specific network, system or application. Most intrusion detection tools not only detect attacks, but also software misuse, policy violations and other forms of inappropriate activities.

A Host-based IDS performs intrusion detection from within the systems you want to protect. Some of these tools perform log analysis, others spyware detection, while others perform virus detection.

LIDS LIDS (Log-based intrusion detection systems) is just a fancy term for tools that perform security log analysis (specified above). It's goal is to detect misuse (or attacks) using logs as the primary source of information. It is not a replacement for NIDS (Network-based IDS) or any other security solution, but an addition to them.

CHAPTER 3

Indices and tables

- *genindex*
- *modindex*
- *search*