

# Linux Network Security, Troubleshooting & Tips

PRESENTER

Ray Hunter  
(bigdog)

Senior Software Engineer  
Northrop Grumman

System Architecture and Administration  
Contractor

# Presentation Outline

- Troubleshooting with Syslog
- Linux Boot Process
- Apache Web Server

# Troubleshooting with Syslog

- What is Syslog?
- Syslog Configuration
- System Monitoring
- What is Logrotate?
- Logrotate Configuration

# What is Syslog?

- Syslog is a utility that is used to log system messages. These messages can be grouped in certain levels and areas.
- When a message is sent to syslog it has 2 descriptive labels:
  - First label is the facility (function) of the application.
  - Second label describes the degree of severity that the message has.
- The message also contains the logging message as well.

# Syslog Facilities

<b>Severity</b>	<b>Keyword</b>	<b>Description</b>
0	Emergencies (EMERG)	System is unusable
1	Alerts (ALERT)	Action must be taken immediately
2	Critical (CRIT)	Critical conditions
3	Errors (ERR)	Error Conditions
4	Warnings (WARNING)	Warning Conditions
5	Notifications (NOTICE)	Normal but significant condition
6	Informational (INFO)	Informational messages
7	Debugging (DEBUG)	Debug-level messages

Levels defined in <linux/kernel.h> header file.

# Syslog Configuration

- Syslog configuration file: `/etc/syslog.conf`
- First part defines the what to log.
- Second part defines where to log.

```
# syslog.conf file
```

```
...
```

```
.info;mail.none;authpriv.none;cron.none /var/log/messages
```

# Syslog Options

- Setting up syslog to log debug information:
- \*.debug /var/log/debug
  
- Setting up syslog to log to a syslog server.
- \*.debug @syslog-host

# System Monitoring

- Restart syslog server after modification to config file.
- Commands:
  - `tail -f /var/log/debug`
  - `grep <string> /var/log/debug | less`
  - `less /var/log/debug`

# What is Logrotate?

- A utility that rotates files based on configuration file directives for those files.
- This allows the user to then assign log rotation that happens on a periodic basis.
- Allows log files to be rotated out, increasing disk space usage.

# Logrotation Configuration

- Configuration of logrotate is done in the `/etc/logrotate.conf` file.
- Additional logrotate scripts can be placed in a directory and loaded via the configuration file.
- Typical directory for logrotate scripts is in the `/etc/logrotate.d/` directory.
- Example: `/etc/logrotate.d/php`

# Logrotate Configuration

- Logrotate configuration file:

```
/path/to/log/file {  
    daily  
    compress  
    create 660 www www  
    notifempty  
    rotate 7  
    missingok  
}
```

# Logrotate Addition Options

- Cron logrotate to rotate log files
- Additional options are many. But some of my favorite are prerotate and postrotate. This allows actions to take place before the rotation and after the rotation.

- For example, a postrotate block

```
postrotate
```

```
kill -HUP `cat /var/run/inn.pid`
```

```
endscript
```

# Linux Boot Process

- Boot loader loads kernel and starts the boot process
- Runs the `/sbin/init` program to start various programs that are needed for the kernel.
- `/sbin/init` then loads the `/etc/inittab` file to determine the system runlevel.
- Based on the default system runlevel `init` will execute the startup scripts located in the proper `/etc/rc.d` subdirectory.
- File names start with 'S' or 'K'. Number after the 'S' or 'K' signifies the order.

# Symbolic Links and Run Levels

- All the init scripts are usually keep in the “/etc/init.d” directory and are symbolically linked from the appropriate directory.
- Runlevels:

<b><i>Mode / Runlevel</i></b>	<b><i>Directory</i></b>	<b><i>Description</i></b>
0	/etc/rc.d/rc0.d	Halt
1	/etc/rc.d/rc1.d	Single User Mode
2	/etc/rc.d/rc2.d	Not Used (can be user defined)
3	/etc/rc.d/rc3.d	Full multiuser mode (no X server)
4	/etc/rc.d/rc4.d	Bigdog's mode
5	/etc/rc.d/rc5.d	Full multiuser mode (with X server)
6	/etc/rc.d/rc6.d	Reboot (ctrl+alt+delete)

# Additional Commands

- init command

```
$ init 0 (halt)
```

```
$ init 6 (reboot)
```

```
$ init 1 (single user)
```

```
$ init 3 (multiuser no x)
```

- chkconfig command

- Utility to change the runlevels for a package

```
$ chkconfig --list | grep sshd
```

```
$ chkconfig --level 01246 sshd off
```

# Outline - Apache Web Server

- Troubleshooting Apache web server
- Virtual Hosts

# Troubleshooting Apache

- Most errors will appear when apache starts.
- Check log files and syslog files for additional information.
- Most errors are syntax errors in configuration file(s).
- Verify that apache is running and listening on the correct port.
- If you can connect to port 80, but the site does not display there is an issues with the website set up.

# Troubleshooting Apache (cont.)

- **Browser 403 Forbidden Error Message**
  - Means there is a permissions issue.
  - Check `/var/log/messages` log file for 'acf: denied' messages.
- **ServerName Error**
  - Configuration file is not set up for the server name properly. `ServerName` directive needs to have a resolvable DNS name.
  - Usually can add `localhost` if testing.

# Apache Log File Layout

- Example access\_log file entry:

```
127.0.0.1 - - [07/Jun/2005:14:28:41 -0600] "GET / HTTP/1.1" 200 46251
```

Field 1: Ip Address

Field 2: Timestamp

Field 3: http query including web page served

Field 4: http result code

Field 5: data sent in bytes

Field 6: webpage that contained the link to the page served (not here)

Field 7: version of web browser used to request the web page (not here)

# Basic HTTP Status Codes

- 200 – Successful request
- 401 – Unauthorized access
- 403 – Forbidden access
- 404 – Page not found
- 500 – Internal server error

# Apache Virtual Hosts

- Named Virtual Hosting
  - Use the NameVirtualHost directive
  - Use the VirtualHost directive to associate names with file locations
- IP-Based Virtual Hosting
  - No usage of the NameVirtualHost directive
  - Only one VirtualHost directive per IP address

# Named Virtual Hosting Example

```
NameVirtualHost 192.168.150.2
<VirtualHost *>
  DocumentRoot /var/www/localhost
</VirtualHost>
<VirtualHost 192.168.150.2>
  servername www.bigdog1.com
  DocumentRoot /var/www/bigdog2
</VirtualHost>
<VirtualHost 192.168.150.2>
  servername www.bigdog2.com
  DocumentRoot /var/www/bigdog2
</VirtualHost>
```

# IP-Based Virtual Hosting Ex.

```
<VirtualHost *>  
  DocumentRoot /var/www/localhost  
</VirtualHost>  
<VirtualHost 192.168.150.2>  
  DocumentRoot /var/www/bigdog1  
</VirtualHost>  
<VirtualHost 192.168.150.3>  
  DocumentRoot /var/www/bigdog2  
</VirtualHost>
```