Diploma in Infocomm & Security

IT2654: Systems Administration & Security

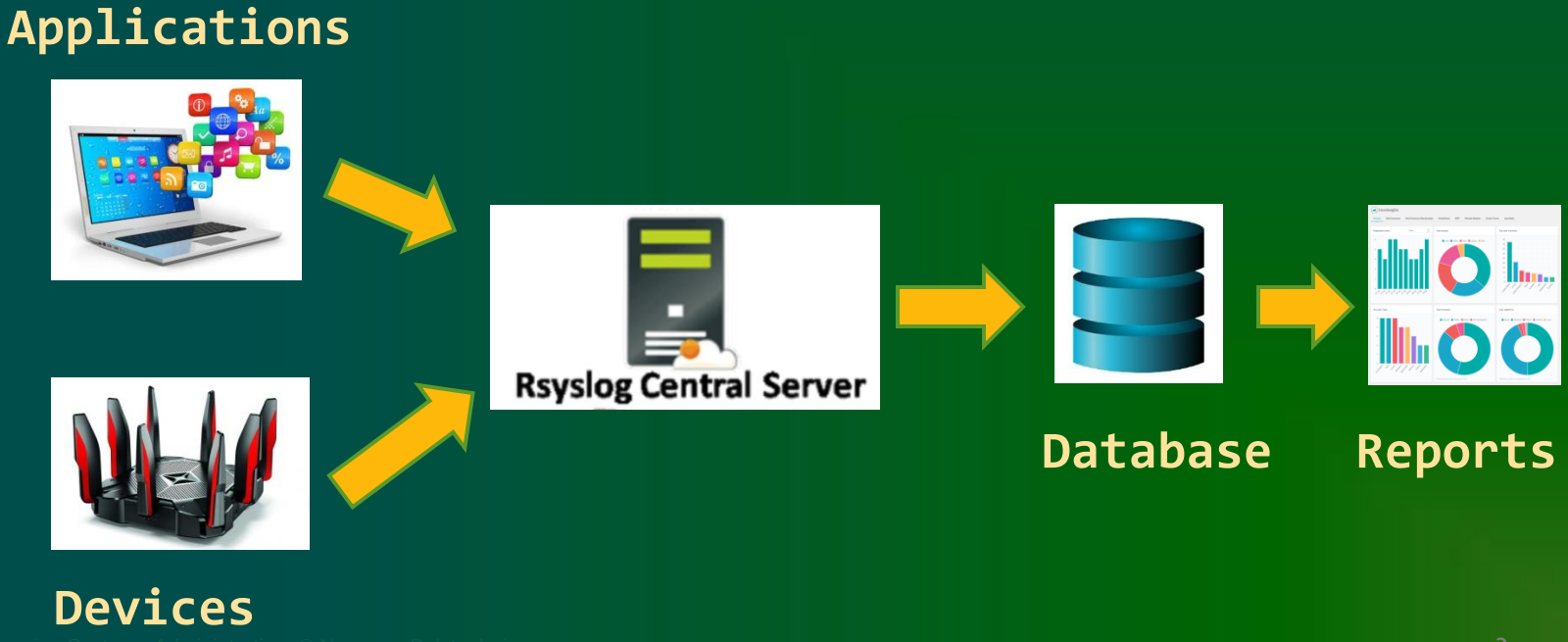
TOPIC 6:
SYSLOG AND LOG FILES

Objectives

- What is logging?
- Benefits of logging
- Linux syslog
  - Syslog Format
  - Redhat syslog configuration

What is logging?

- Logging is the act of keeping a history of events.
- Software (eg. applications) and hardware (eg. routers) can generate logs.



Benefits of Logging

1) Helps to analyze the root cause for any trouble or problems
2) Reduce overall downtime by helping to troubleshoot issues faster with all the logs
3) Improves incident management by active detection of issues
4) Self-determination of incidents along with auto resolution
5) Adhere to legal requirements (ie. address cyber crime)

Component of Syslog Server

1) A Syslog listener (software) – The listener gathers and processes syslog data sent over UDP port 514. There is no acknowledgment of receipt and messages aren't guaranteed to arrive.
2) A database – Syslog servers need databases to store the massive amounts of data for quick access.
3) Management and filtering software – Since there are enormous amounts of data, the database software helps to filter, search data and generate reports.

The Syslog Format

- Syslog has a standard definition and format of the log message defined by RFC 5424.
- It is composed of a header, structured-data (SD) and a message.
- The header can consists of the following:

  - Priority
  - Version
  - Timestamp
  - Hostname
  - Application
  - Process id
  - Message id

The Syslog Format

- The structured-data have data blocks in the "key=value" format within square brackets.

For example, the following message:

```
<34>1 2003-10-11T22:14:15.003Z mymachine.example.com su - ID47 - BOM'su root' failed for lonvick on /dev/pts/8
```

Corresponds to the following format:

```
<priority>VERSION ISOTIMESTAMP HOSTNAME APPLICATION PID MESSAGEID STRUCTURED-DATA MSG
```

The Syslog Format

- Syslog messages are used to report levels of Emergency and Warnings with regards to software or hardware issues.
- Syslog has these message levels:
  1) **Emergency Messages** – System is unavailable and unusable (Could be a “panic” condition due to a natural disaster)
  2) **Alert Messages** – Action needs to be taken immediately (an example is loss of backup ISP connection)
  3) **Critical Messages** – Critical conditions (this could be a loss of primary ISP connection)
  4) **Error Messages** – Error conditions (must be resolved within a specified time frame)
  5) **Warning Messages** – Warning conditions (indicates an error may occur if action is not taken)
  6) **Notification Messages** – Things are normal, but this is still a significant condition (immediate action is usually not required)
  7) **Informational Messages** – Informational messages (for reporting and measuring)
  8) **Debugging Messages** – Debug-level messages (Offers information around debugging apps)

Redhat Configuration

- The main configuration file for syslog is
  - `/etc/rsyslog.conf`
- All log files store in /var/log directory by default
- The **syslogd** daemon* uses the rsyslog.conf file to execute the logs
- The rsyslog.conf specifies rules for logging.
- Every rule has two fields – a SELECTOR field and an ACTION field.

▶ *Selector* <TAB> *action*

▶ eg. mail.info /var/log/maillog

Linux Daemon

A daemon is a type of program on Unix-like operating systems that runs unobtrusively in the background, rather than under the direct control of a user, waiting to be activated by the occurrence of a specific event or condition.

Selector Field

- The selector field specifies a pattern of facilities and priorities belonging to the specified action.
- The selector field consists of two parts, a **FACILITY** and a **PRIORITY**, separated by a period ("."). Both parts are case insensitive.
  - source -- the program (‘facility’) that is sending a log message
  - importance -- the messages' severity level
  - eg. mail.info /var/log/maillog

Facility Keywords

Keyword	Facility	Description
0	kern	kernel messages
1	user	user level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9	clock daemon	
10	authpriv	security/authorization messages
11	ftp	FTP daemon

Facility Keywords

Keyword	Facility	Description
12	-	NTP susbsystem
13	-	log audit
14	-	log alert
15	cron	clock daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)
20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

Severity / Priority Level

Level	Approximate meaning
emerg (panic)	Panic situation
alert	Urgent situation
crit	Critical situation
err	Other error conditions
warning	Warning messages
notice	Unusual things that may need investigation
info	Informational messages
debug	For debugging

Examples of Rules

Log all the critical events on your Linux machine in a separate log file inside /var/log with a name of critical.log

Append this line inside `/etc/syslog.conf`

```
*.=crit          /var/log/critical.log
```

Log all the kernel related messages in separate log file inside /var/log /firewall.log

Add a new line

```
Kern.*      /var/log/firewall.log
```

Important Log Files

- These are some of high priority log files you should monitor:
  - /var/log/messages – Contains most system messages
  - /var/log/secure – Authentication messages
  - /var/log/cron – Logs Cron job activities
  - /var/log/maillog – Mail transactions

Rotating Log Files

- Linux can rotate a log file once it reaches a particular file size.
- The Unix logrotate utility will continue to write the log information to a new file after rotating the old file.
- Key files are:
  - `/usr/sbin/logrotate – The logrotate command`
  - `/etc/cron.daily/logrotate – The shell script that executes the logrotate command on a daily basis.`
  - `/etc/logrotate.conf – This is used as log rotation for all the log entries in this file`
  - `/etc/logrotate.d – For individual packages`

Summary

- Logging is important in a computer system.
- Software and hardware can generate log files.
- Log files should be centralized for ease of management and control.
- Redhat 6 uses the /etc/rsyslog.conf file to configure syslog