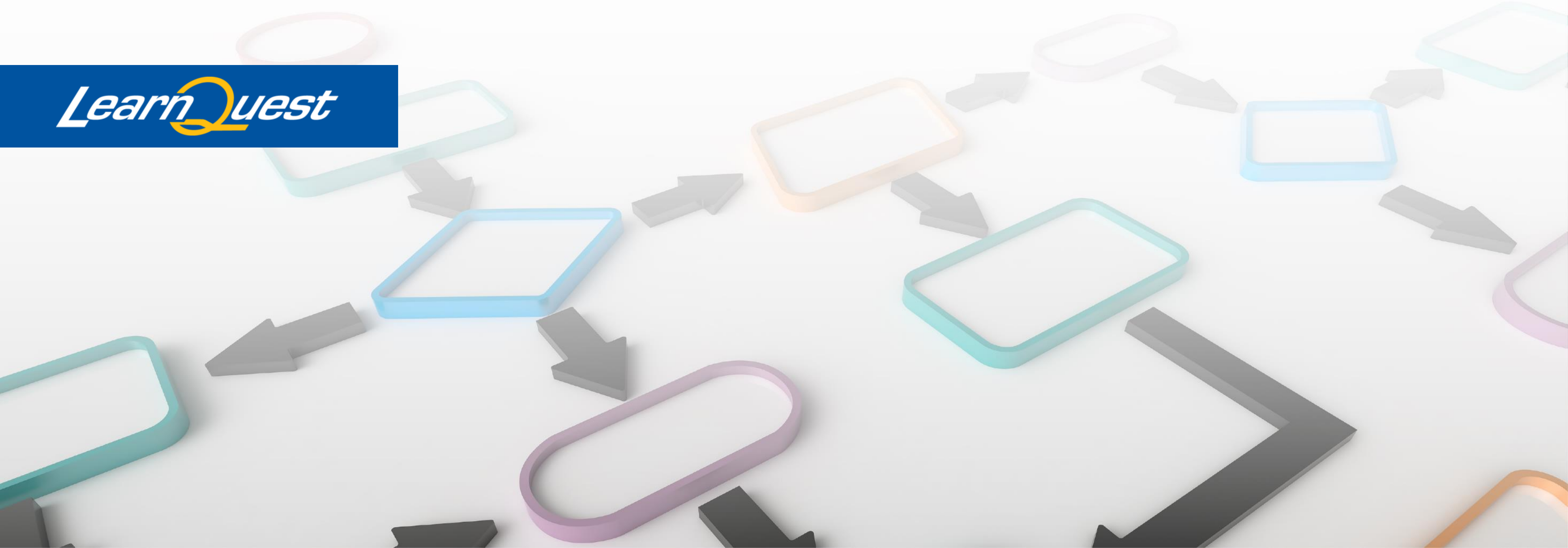
Securing Linux Systems

- 3rd Course in Linux Foundations Specialization



Logging & Backups

In this module, we look at both local and remote system logging. We will also look at backup and compression of the files on the system to allow recovery in response to a system incident.

3

Learning Objectives

Logging & Backups

Upon completion of this module, learners will be able to:

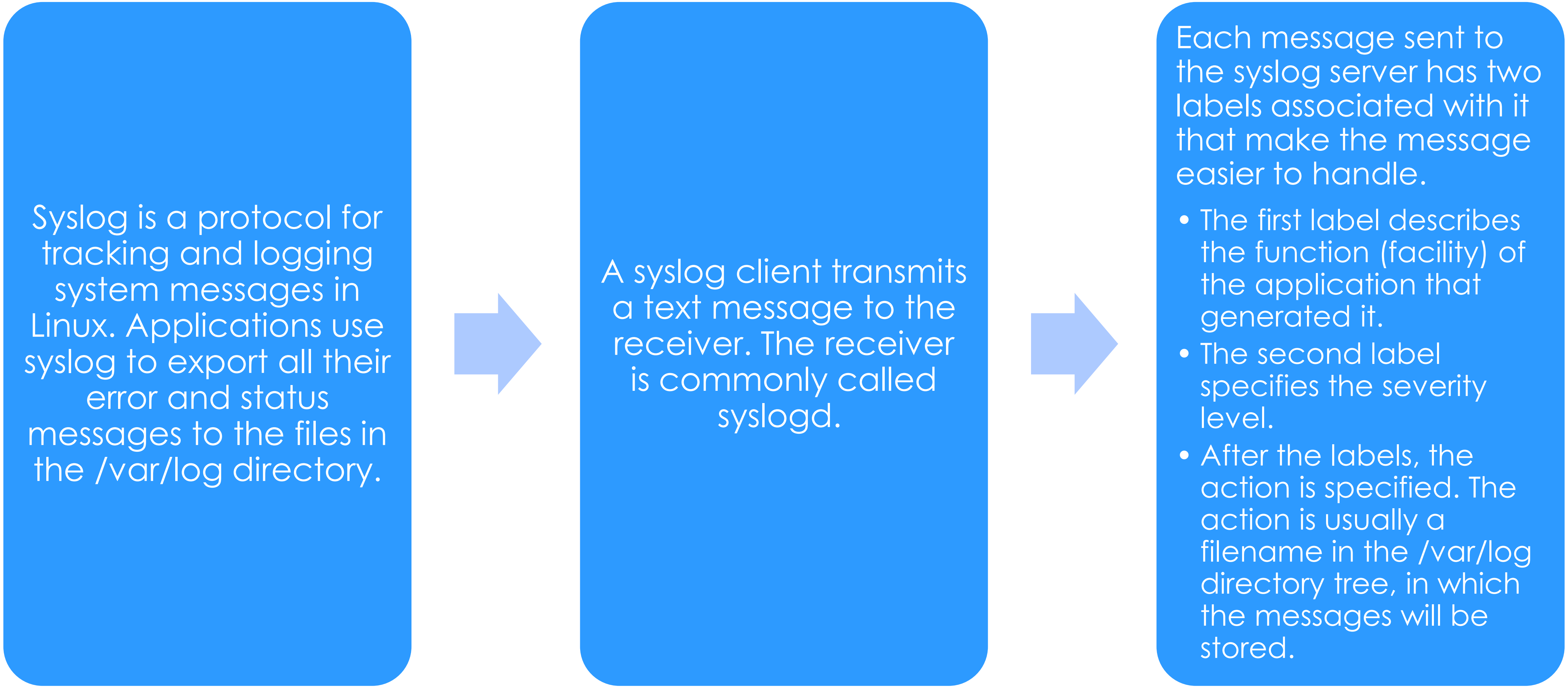
- Describe syslog protocol
- Describe Systemd Journaling
- List Backup types
- Compare archive and restore tools

Lesson 1

System Logging

In this lesson, we look at how Linux handles System Logging

Syslog



Syslog is a protocol for tracking and logging system messages in Linux. Applications use syslog to export all their error and status messages to the files in the /var/log directory.

A syslog client transmits a text message to the receiver. The receiver is commonly called syslogd.

Each message sent to the syslog server has two labels associated with it that make the message easier to handle.

- The first label describes the function (facility) of the application that generated it.
- The second label specifies the severity level.
- After the labels, the action is specified. The action is usually a filename in the /var/log directory tree, in which the messages will be stored.

Syslog Protocol Facility Values

Number	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
12	–	NTP subsystem
13	–	log audit
14	–	log alert
15	cron	clock daemon
16-23	local0-7	local use

Syslog Severity Levels

Code	Severity	Keyword	Description
0	Emergency	emerg (panic)	System is unusable.
1	Alert	alert	Action must be taken immediately.
2	Critical	crit	Critical conditions.
3	Error	err (error)	Error conditions.
4	Warning	warning (warn)	Warning conditions.
5	Notice	notice	Normal but significant condition.
6	Informational	info	Informational messages.
7	Debug	debug	Debug-level messages.

Lesson 1 Review

Syslog is a protocol for tracking and logging system messages

The first label defines the function that generated the activity being logged

The second label defines the severity of the issue that generated the activity being logged

Lesson 2

Systemd Journaling

In this lesson, we look at the Systemd Journal

Systemd Journal

The journal is a component of systemd.

A centralized location for all messages logged by different components in a systemd-enabled Linux system.

Includes kernel and boot messages, messages coming from syslog, or different services.

Journal Location

Storage setting determines how systemd-journald stores event messages

- Auto - will look for the /var/log/journal directory and store event messages there.
  - If that directory doesn’t exist, it stores the event messages in the temporary /run/log/journal directory, which is deleted when the system shuts down.
  - You must manually create the /var/log/journal directory for the event messages to be stored permanently.
- Persistent - systemd-journald will create the directory automatically.
- Volatile - stores event messages in the temporary directory.

Journal Configuration

Compress setting determines whether to compress the journal files.

There are several file maintenance settings that control how much space the journal is allowed to use as well as how often to split journal files for archive, based on either time or file size.

The ForwardToSyslog setting determines if systemd-journald should forward any received messages to a separate syslog program, such as rsyslogd, running on the system.

Lesson 2 Review

Systemd Journaling is the standard journaling of Systemd distros

Configuration allows you to control where the journal is created

Configuration allows you to control how the journal is compressed and split across files

Lesson 3

Backups

In this lesson we the drill into backup types

Backup Type

System Image - A system image is a copy of the operating system binaries, configuration files, and anything else you need to boot the Linux system.

Full - A full backup is a copy of all the data, ignoring its modification date.

Incremental - An incremental backup only makes a copy of data that has been modified since the last backup operation.

Differential - A differential backup makes a copy of all data that has changed since the last full backup.

Snapshot - A full copy of the data is made to backup media. Then pointers are employed to create a reference table linking the backup data with the original data. The next time a backup is made, an incremental backup occurs, and the pointer reference table is copied and updated.

Snapshot Clone - Once a snapshot is created, such as an LVM snapshot, it is copied, or cloned.

Compression Tools

1

gzip - Uses the Lempel-Ziv (LZ77) algorithm to achieve text-based file compression rates of 60–70%

2

bzip2 - Offers higher compression rates than gzip but takes slightly longer to perform the data compression.

3

xz - Higher default compression rate than bzip2 and gzip via the LZMA2 compression algorithm.

4

zip - Different from the other data compression utilities in that it operates on multiple files.

Lesson 3 Review

A system backup is designed to restore to a bootable system

A full backup includes all the files and directories

An incremental backup includes just files changed since last backup

Lesson 4

Archive and Restore Tools

In this lesson, we look at how to archive backups

Archive and Restore Utilities

Archiving is the process of combining multiple files and directories into one file.

Compression is the process of reducing the size of a file or directory.

Archiving is usually used as part of a system backup or when moving data from one system to another.

There are four archive tools we will discuss here:

- cpio
- dd
- rsync
- tar

Cpio Command

The cpio utility’s name stands for “copy in and out.”.

Example Usage:

```
ls my*.txt | cpio -ov > mybak.cpio
```

Options:

-i : Extract

-o: Create

-t : List

Tar Command

The tar utility’s name stands for tape archiver.

Example Usage:

- tar -cvf mybak.tar my*.txt

Options:

- -c : Create
- -j: Use bzip2 compression
- -J: Use xz compression
- -v: Verbose
- -x: Extract
- -z : Use gzip compression

Dd Command

The dd utility allows you to back up nearly everything on a disk.

Example Usage:

- dd if=/dev/sda of=/dev/sdb status=progress

Options:

- if: input file
- of: output file
- status: level of information to display to STDERR

Rsync Command

Copy files locally or remotely

Example Usage:

```
rsync -av /home/aspeno /home/bkup
```

Options:

-a : Create an Archive

-v: Verbose

-z : Use compression

Lesson 4 Review

Archiving is the process of combining multiple files and directories into one file

Compression is the process of reducing the size of a file or directory

Archiving is usually used as part of a system backup or when moving data from one system to another