Module-8: The Useful DevOps Tools & Commands

Assignment Solution

Version 2.0

1) What is rsyslog service? How it can be configured?

Rsyslog is a system utility providing support for message logging. Every logged message contains at least a time and a hostname field, normally a program name field, too, but that depends on how trusty the logging program is. The rsyslog package supports free definition of output formats via templates. It also supports precise timestamps and writing directly to databases.

/etc/syslog.conf: Configuration file for rsyslogd. See rsyslog.conf (5) for exact information.

/dev/log: The Unix domain socket to from where local syslog messages are read.

/var/run/rsyslogd.pid: The file containing the process id of rsyslogd.

prefix/lib/rsyslog: Default directory for rsyslogd modules. The prefix is specified during compilation (e.g. /usr/local).

-d Turns on debug mode. Using this the daemon will not proceed a

fork(2) to set itself in the background, but opposite to that

stay in the foreground and write much debug information on the

current tty. See the DEBUGGING section for more information.

-f config file

Specify an alternative configuration file instead of

/etc/rsyslog.conf, which is the default.

-i pid file

Specify an alternative pid file instead of the default one.

This option must be used if multiple instances of rsyslogd should run on a single machine.

-l hostlist

Specify a hostname that should be logged only with its simple hostname and not the fqdn. Multiple hosts may be specified using the colon (``:'') separator.

-n Avoid auto-backgrounding. This is needed especially if the rsyslogd is started and controlled by init(8).

-N level

Do a coNfig check. Do NOT run in regular mode, just check configuration file correctness. This option is meant to verify a config file. To do so, run rsyslogd interactively in foreground, specifying -f <config-file> and -N level. The level argument modifies behaviour. Currently, 0 is the same as not specifying the -N option at all (so this makes limited sense) and 1 actually activates the code. Later, higher levels will mean more verbosity (this is a forward-compatibility option). rsyslogd is started and controlled by init(8).

-q add hostname if DNS fails during ACL processing

During ACL processing, hostnames are resolved to IP addresses for performance reasons. If DNS fails during that process, the hostname is added as wildcard text, which results in proper, but somewhat slower operation once DNS is up again.

-Q do not resolve hostnames during ACL processing

Do not resolve hostnames to IP addresses during ACL processing.

-s domainlist

Specify a domain name that should be stripped off before logging. Multiple domains may be specified using the colon (``:'') separator. Please be advised that no sub-domains may be specified but only entire domains. For example if -s north.de is specified and the host logging resolves to satu.infodrom.north.de no domain would be cut, you will have to specify two domains like: -s north.de:infodrom.north.de.

-S ip_addresslocal client source IP

rsyslogd uses ip_address as local client address while connecting to remote logserver. Currently used by omrelp only and only with tcp.

-u userlevel

This is a "catch all" option for some very seldomly-used user settings. The "userlevel" variable selects multiple things. Add the specific values to get the combined effect of them. A value of 1 prevents rsyslogd from parsing hostnames and tags inside messages. A value of 2 prevents rsyslogd from changing to the root directory. This is almost never a good idea in production use. This option was introduced in support of the internal testbed. To combine these two features, use a userlevel of 3 (1+2). Whenever you use an -u option, make sure you really understand what you do and why you do it.

-v Print version and exit.

-w Suppress warnings issued when messages are received from non-authorized machines (those, that are in no AllowedSender list).

-x Disable DNS for remote messages.

2. What is the Benefits Audit system on the server? How can it be done?

It's responsible for writing audit records to the disk. Viewing the logs is done with the auditd ausearch or aureport utilities. audit helps make your system more secure by providing you with a means to analyze what is happening on your system in great detail. Audit is useful for tracking issues and helps taking additional security measures, configuring the audit rules is done with the auditctl utility. During startup, the rules in /etc/audit/audit.rules are read by auditctl. The audit daemon itself has some configuration options that the admin may wish to customize. They are found in the auditd.conf file.

In order to use audit facility you need to use following utilities
=> **auditctl** - a command to assist controlling the kernel's audit system. You can get status, and add or delete rules into kernel audit system. Setting a watch on a file is accomplished using this command:
=> **ausearch** - a command that can query the audit daemon logs based for events based on different search criteria.
=> **aureport** - a tool that produces summary reports of the audit system logs.

Review the Audit Trail

Linux audit provides tools that write the audit reports to disk and translate them into human readable format.

Review Particular Audit Events

Audit provides a utility that allows you to filter the audit reports for certain events of interest. You can filter for:

- User
- Group
- Audit ID
- Remote Hostname
- Remote Host Address
- System Call
- System Call Arguments
- File
- File Operations
- Success or Failure

Apply a Selective Audit

Audit provides the means to filter the audit reports for events of interest and also to tune audit to record only selected events. You can create your own set of rules and have the audit daemon record only those of interest to you.

Guarantee the Availability of the Report Data

Audit reports are owned by root and therefore only removable by root. Unauthorized users cannot remove the audit logs.

Prevent Audit Data Loss

If the kernel runs out of memory, the audit daemon's backlog is exceeded, or its rate limit is exceeded, audit can trigger a shutdown of the system to keep events from escaping audit's control. This shutdown would be an immediate halt of the system triggered by the audit kernel component without any syncing of the latest logs to disk. The default configuration is to log a warning to syslog rather than to halt the system.

If the system runs out of disk space when logging, the audit system can be configured to perform clean shutdown (init 0). The default configuration tells the audit daemon to stop logging when it runs out of disk space.

3) What is Nagios and what are its advantages?

Nagios is an open source computer system monitoring, network monitoring and infrastructure monitoring software application. Nagios is used for monitoring and alerting services for servers, switches, applications, and services. It send alerts to users when things go wrong and alerts them a second time when the issue is resolved.

Monitoring of network services

Monitoring of host resources (processor load, disk usage, system logs)

Monitoring via remotely run scripts via Nagios Remote Plugin Executor

Remote monitoring supported through SSH or SSL encrypted tunnels.

A simple plugin design that allows users to easily develop their own service checks depending on needs

Available data graphing plugins

Parallel service checks

The ability to define network host hierarchies using 'parent' hosts, allowing the detection of and distinction between hosts that are down or unreachable

Contact notifications when service or host problems occur and get resolved (via e-mail, pager, SMS, or any user-defined method through plugin system)

4) What is the importance of fstab file?

/etc/fstab file is used to control what file systems are mounted when the system boots, as well for other file systems that may be mounted manually from time to time.

Each line represents one file system and contains the following fields:

- File system specifier -- For disk-based file systems, either a device file name (/dev/sda1), a file system label specification (LABEL=/), or a devlabel-managed symbolic link (/dev/homedisk)
- Mount point -- Except for swap partitions, this field specifies the mount point to be used when the file system is mounted (/boot)

- File system type -- The type of file system present on the specified device (note that auto may be specified to select automatic detection of the file system to be mounted, which is handy for removable media units such as diskette drives)
- Mount options -- A comma-separated list of options that can be used to control mount's behavior (noauto, owner, kudzu)
- Dump frequency -- If the dump backup utility is used, the number in this field controls dump's handling of the specified file system
- File system check order -- Controls the order in which the file system checker fsck checks the integrity of the file systems

5) What are the **different commands** network statistics?

The different commands for network statistics are

netstat - prints information about the Linux networking subsystem. It lists out all the tcp, udp socket connections and the unix socket connections. Apart from connected sockets it can also list listening sockets that are waiting for incoming connections. The type of information printed is controlled by the first argument, as follows:

(none) By default, netstat displays a list of open sockets. If you don't specify any address families, then the active sockets of all configured address families will be printed.

--route, -r Display the kernel routing tables.

--groups, -g Display multicast group membership information for IPv4 and IPv6.

--interface=*iface* , -I Display a table of all network interfaces, or the specified *iface.*

--statistics, -s Display summary statistics for each protocol.

sar

Using sar you can monitor performance of various Linux subsystems. The **sar** command extracts and writes to standard output records previously saved in a file. This file can be either the one specified by the **-f** flag or, by default, the standard system activity daily data file.

monitor the following Linux performance statistics using sar.

1. Collective CPU usage
2. Individual CPU statistics
3. Memory used and available
4. Swap space used and available
5. Overall I/O activities of the system
6. Individual device I/O activities
7. Context switch statistics
8. Run queue and load average data
9. Network statistics
10. Report sar data from a specific time

iostat

iostat reports Central Processing Unit (CPU) statistics and input/output statistics for devices and partitions. The iostat command is used for monitoring system input/output device loading by observing the time the devices are active in relation to their average transfer rates. The iostat command generates reports that can be used to change system configuration to better balance the input/output load between physical disks. The report consists of a CPU header row followed by a row of CPU statistics. On multiprocessor systems, CPU statistics are calculated system-wide as averages among all processors.

The iostat command generates three types of reports: the CPU Utilization report, theDevice Utilization report and the Network Filesystem report.