How to Setup an Enterprise Level Central Logging Service

Motivation

The fun of a new job. You get to earn your spurs again and again until you've proven yourself to your new team. At my new job, one of the things sorely lacking is a solution for central logging (for the OS level and application level). My goal of this exercise is to bring together both of these logs (OS and app) into a central database that will allow me to write custom queries to discover: misconfigurations, new servers and services, unauthorized services, and hardware/software precursors to failure (meaning the tell-tell warning signs of impending failures that are often ignored until after a catastrophic disaster in the data center).

Test environment layout

The operating systems will be CentOS 6.5 for both the logging server and one web application server running Jboss AS version 7.0. Both were installed and configured inside of VMware Workstation version 10.0. VMware led the OS install, similar to kickstart without user intervention (meaning that when I turned on the VM for the first time, VMware automated the install of the operating system without user input).

Setup and deployment

Install the LAMP stack (all commands below assume you are logged on as root):

```
# umask 0022
# yum install httpd -y
# service httpd start
# chkconfig httpd on
```

Modify iptables to look like this:

```
# vi /etc/sysconfig/iptables

My Output:
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
```

```
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 514 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Install MariaDB:

```

# yum remove mysql* mysql-server mysql-devel mysql-libs
# rpm -ivh http://rpms.famillecollet.com/enterprise/remi-release-6.rpm
# yum --enablerepo=remi-test --disablerepo=remi install compat-mysql55

# vi /etc/yum.repos.d/mariadb.repo

My Output:
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/5.5/centos6-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1

# yum clean all
# yum update

# yum install MariaDB-devel MariaDB-client MariaDB-server -y
# service mysql start
# chkconfig mysql on
```

Set the MySQL Password:

```
# /usr/bin/mysql_secure_installation
```

Install PHP:

```
# yum install php phpmyadmin -y
# service httpd restart
# cat <<-EOF>/var/www/html/testphp.php
<html>
<head>
<title> PHP Test Script </title>
</head>
<body>
<?php
phpinfo( );
?>
</body>
</html>
```

Use your web browser to test: http://<your_ip>/testphp.php

Install Rsyslog:

```
# yum install rsyslog*
# service rsyslog status
# chkconfig rsyslog on
```

Modify the database schema script:

```
# cp /usr/share/doc/rsyslog-mysql-5.8.10/createDB.sql /root/
# vi /root/createDB.sql
```

Change these two lines to:

```
CREATE DATABASE rsyslogdb;
USE rsyslogdb;
```

Import the script into MySQL:

```
# mysql -u root -p < /root/createDB.sql
```

Set user permissions inside the DB:

```
# mysql -u root -p
> GRANT ALL ON rsyslogdb.* TO rsysloguser@localhost IDENTIFIED BY 'centos';
> flush privileges;
> exit
```

Modify the Rsyslog configuration:

```
# vi /etc/rsyslog.conf
## uncomment ##
$ModLoad imudp
$UDPServerRun 514
# Provides TCP syslog reception
## Uncomment ##
$ModLoad imtcp
$InputTCPServerRun 514

## Add the following lines ##
$ModLoad ommysql
$ModLoad ommysql
*.* :ommysql:127.0.0.1,rsyslogdb,rsysloguser,centos
$AllowedSender UDP, 127.0.0.1, 192.168.139.0/24
$AllowedSender TCP, 127.0.0.1, 192.168.139.0/24
```

Where:

rsyslogdb:	**The** database name
rsysloguser:	**The** database username
centos:	**The** rsyslog user password

$AllowedSender: Where rsyslog accepts logs from clients on both UDP and TCP ports.

Install LogAnalyzer:

```
# wget http://download.adiscon.com/loganalyzer/loganalyzer-3.6.5.tar.gz
# tar zxvf loganalyzer-3.6.5.tar.gz
# mv loganalyzer-3.6.5/src/ /var/www/html/loganalyzer
# mv loganalyzer-3.6.5/contrib/* /var/www/html/loganalyzer/
# cd /var/www/html/loganalyzer/
# chmod +x configure.sh secure.sh
# ./configure.sh
```

Disable SELinux:

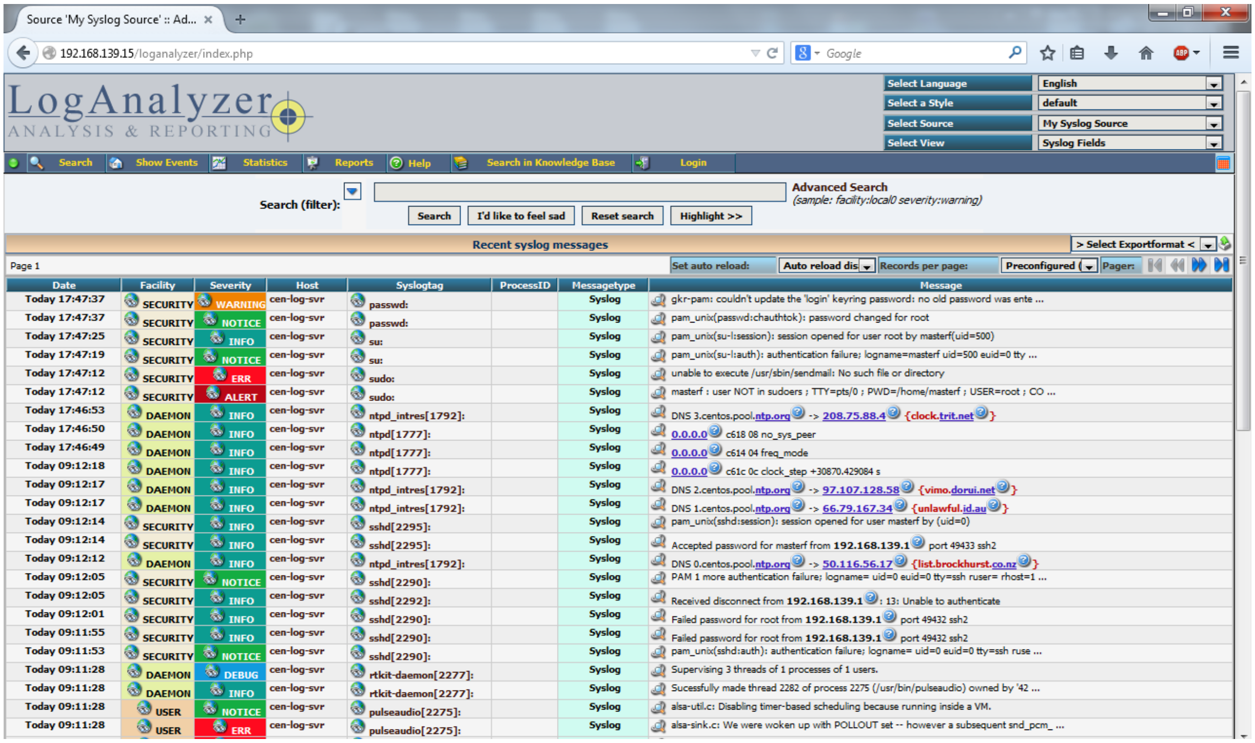
```
# vi /etc/sysconfig/selinux
```

Change **SELINUX=enforcing** to **SELINUX=disabled**

GUI Configuration of LogAnalyzer

Point your web browser to **http://ip-address/loganalyser** or **http://domain-name/loganalyzer** and begin LogAnalyzer installation.
You'll be shown with an Error message that says: Critical Error occurred.
Click on link that says: **'here'**.

Follow the web install using the default values presented.



Select Language: English
Select a Style: default
Select Source: My Syslog Source
Select View: Syslog Fields

Search (filter):

Page 1

Set auto reload: Auto reload dis
Records per page: Preconfigured (

Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 17:47:37	SECURITY	WARNING	cen-log-svr	passwd:		Syslog	gkr-pam: couldn't update the 'login' keyring password: no old password was ente ...
Today 17:47:37	SECURITY	NOTICE	cen-log-svr	passwd:		Syslog	pam_unix(passwd:chauthtok): password changed for root
Today 17:47:25	SECURITY	INFO	cen-log-svr	su:		Syslog	pam_unix(su-l:session): session opened for user root by masterf(uid=500)
Today 17:47:19	SECURITY	NOTICE	cen-log-svr	su:		Syslog	pam_unix(su-l:auth): authentication failure; logname=masterf uid=500 euid=0 tty ...
Today 17:47:12	SECURITY	ERR	cen-log-svr	sudo:		Syslog	unable to execute /usr/sbin/sendmail: No such file or directory
Today 17:47:12	SECURITY	ALERT	cen-log-svr	sudo:		Syslog	masterf : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/masterf ; USER=root ; CO ...
Today 17:46:53	DAEMON	INFO	cen-log-svr	ntpd_intres[1792]:		Syslog	DNS 3.centos.pool.ntp.org -> 208.75.88.4 {clock.trit.net}
Today 17:46:50	DAEMON	INFO	cen-log-svr	ntpd[1777]:		Syslog	0.0.0.0 c618 08 no_sys_peer
Today 17:46:49	DAEMON	INFO	cen-log-svr	ntpd[1777]:		Syslog	0.0.0.0 c614 04 freq_mode
Today 09:12:18	DAEMON	INFO	cen-log-svr	ntpd[1777]:		Syslog	0.0.0.0 c61c 0c clock_step +30870.429084 s
Today 09:12:17	DAEMON	INFO	cen-log-svr	ntpd_intres[1792]:		Syslog	DNS 2.centos.pool.ntp.org -> 97.107.128.58 {vimo.dorui.net}
Today 09:12:17	DAEMON	INFO	cen-log-svr	ntpd_intres[1792]:		Syslog	DNS 1.centos.pool.ntp.org -> 66.79.167.34 {unlawful.id.au}
Today 09:12:14	SECURITY	INFO	cen-log-svr	sshd[2295]:		Syslog	pam_unix(sshd:session): session opened for user masterf by (uid=0)
Today 09:12:14	SECURITY	INFO	cen-log-svr	sshd[2295]:		Syslog	Accepted password for masterf from 192.168.139.1 port 49433 ssh2
Today 09:12:12	DAEMON	INFO	cen-log-svr	ntpd_intres[1792]:		Syslog	DNS 0.centos.pool.ntp.org -> 50.116.56.17 {list.brockhurst.co.nz}
Today 09:12:05	SECURITY	NOTICE	cen-log-svr	sshd[2290]:		Syslog	PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1 ...
Today 09:12:05	SECURITY	INFO	cen-log-svr	sshd[2292]:		Syslog	Received disconnect from 192.168.139.1: 13: Unable to authenticate
Today 09:12:01	SECURITY	INFO	cen-log-svr	sshd[2290]:		Syslog	Failed password for root from 192.168.139.1 port 49432 ssh2
Today 09:11:55	SECURITY	INFO	cen-log-svr	sshd[2290]:		Syslog	Failed password for root from 192.168.139.1 port 49432 ssh2
Today 09:11:53	SECURITY	NOTICE	cen-log-svr	sshd[2290]:		Syslog	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruse ...
Today 09:11:28	DAEMON	DEBUG	cen-log-svr	rtkit-daemon[2277]:		Syslog	Supervising 3 threads of 1 processes of 1 users.
Today 09:11:28	DAEMON	INFO	cen-log-svr	rtkit-daemon[2277]:		Syslog	Sucessfully made thread 2282 of process 2275 (/usr/bin/pulseaudio) owned by '42 ...
Today 09:11:28	USER	NOTICE	cen-log-svr	pulseaudio[2275]:		Syslog	alsa-util.c: Disabling timer-based scheduling because running inside a VM.
Today 09:11:28	USER	ERR	cen-log-svr	pulseaudio[2275]:		Syslog	alsa-sink.c: We were woken up with POLLOUT set -- however a subsequent snd_pcm_ ...

Conclusion

By following these steps, you are able to recreate the process of installing LogAnalyzer. The securing of the product comes from both Iptables securing the ports and the rsyslog configuration itself. For the production environment, I've modified the source IP address range in iptables to match our staging and production servers. For SSH (TCP port 22), limit the source IP address range to your management network. In the application, configure it to only accept packets from the servers in your domain. For the web interface (TCP port 80) you might consider only allowing your sys admins and network administrators to gain access. I allow my developers to access this server so that they can quickly understand how their applications are behaving.

For JBoss, you will need to modify the configuration file, standalone.xml in order to achieve this, restart jboss and test LogAnalyzer for new records. See the Appendix for my configuration.

Appendix

/etc/sysconfig/iptables:

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
```

```
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 514 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

/etc/rsyslog.conf:

```
# rsyslog v5 configuration file
# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# If you experience problems, see
http://www.rsyslog.com/doc/troubleshoot.html
#### MODULES ####
$ModLoad imuxsock # provides support for local system logging (e.g. via
logger command)
$ModLoad imklog   # provides kernel logging support (previously done by
rklogd)
#$ModLoad immark  # provides --MARK-- message capability
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
$ModLoad ommysql
$ModLoad ommysql
*.* :ommysql:127.0.0.1,rsyslogdb,rsysloguser,centos
$AllowedSender UDP, 127.0.0.1, 192.168.139.0/24
$AllowedSender TCP, 127.0.0.1, 192.168.139.0/24
#### GLOBAL DIRECTIVES ####
# Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
# File syncing capability is disabled by default. This feature is usually not
required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on
# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf
#### RULES ####
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages
# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure
# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog
# Log cron stuff
cron.*                                                  /var/log/cron
```

```
# Everybody gets emergency messages
*.emerg                                                 *
# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/spooler
# Save boot messages also to boot.log
local7.*                                                /var/log/boot.log
# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$WorkDirectory /var/lib/rsyslog # where to place spool files
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
# ### end of the forwarding rule ###
#
# A template to for higher precision timestamps + severity logging
$template SpiceTmpl,"%TIMESTAMP%.%TIMESTAMP:::date-
subseconds% %syslogtag% %syslogseverity-text%:%msg:::sp-if-no-1st-
sp%%msg:::drop-last-lf%\n"
#
:programname, startswith, "spice-vdagent"       /var/log/spice-
vdagent.log;SpiceTmpl
```

/root/createDB.sql:

```
CREATE DATABASE rsyslogdb;
USE rsyslogdb;
CREATE TABLE SystemEvents
(
        ID int unsigned not null auto_increment primary key,
        CustomerID bigint,
        ReceivedAt datetime NULL,
        DeviceReportedTime datetime NULL,
        Facility smallint NULL,
        Priority smallint NULL,
        FromHost varchar(60) NULL,
        Message text,
        NTSeverity int NULL,
        Importance int NULL,
        EventSource varchar(60),
        EventUser varchar(60) NULL,
        EventCategory int NULL,
        EventID int NULL,
        EventBinaryData text NULL,
        MaxAvailable int NULL,
        CurrUsage int NULL,
        MinUsage int NULL,
        MaxUsage int NULL,
        InfoUnitID int NULL ,
        SysLogTag varchar(60),
        EventLogType varchar(60),
        GenericFileName VarChar(60),
        SystemID int NULL
);
```

```
CREATE TABLE SystemEventsProperties
(
        ID int unsigned not null auto_increment primary key,
        SystemEventID int NULL ,
        ParamName varchar(255) NULL ,
        ParamValue text NULL
);
```

JBoss Logging

Inside the standalone.xml inside /opt/jboss/default/configuration/standalone.xml:

Add the following handler (the console-handler and the periodic-rotating-file-handler should be there already):

```
<syslog-handler name="SYSLOG">
                <level name="INFO" />
                <server-address value="192.168.139.15" />
                <app-name value="jboss" />
                <hostname value="jboss-staging001" />
            </syslog-handler>
```

Add the syslog handler to the root-handlers:

```
<root-logger>
                <level name="INFO"/>
                <handlers>
                    <handler name="CONSOLE"/>
                    <handler name="FILE"/>
                    <handler name="SYSLOG"/>
                </handlers>
            </root-logger>
```