Forwarding logs from rsyslog client to a remote rsyslogs server

Introduction

This guide will walk you through setting up Rsyslog for log forwarding between a client and a remote server using Linux.

Setup

Server: The machine which will send message
Client: The machine which will receive the message

Prerequisites

Software Requirements

- Linux operating system
- Rsyslog (version 5.0 or higher recommended)
- Root or sudo access

Network Requirements

- Network connectivity between client and remote server
- Known IP address of the remote Rsyslog server
- Open network ports (typically 514 for UDP or TCP)

Step-by-Step Configuration Guide

Preparation

Before beginning, ensure you have:

- Administrative (root) access

- Stable network connection
- IP address of the remote server

Step 1: Rsyslog Installation

1.1 Obtain Root Access

```
sudo -i
```

- Enter your root password when prompted

1.2 Update System Packages

If you are using DNF, use the command below:

```
sudo dnf update
```

If you are using YUM, use the command below:

```
sudo yum update
```

1.3 Install Rsyslog

If you are using YUM, use the command below:

```
sudo yum install rsyslog
```

If you using DNF, use the command below:

```
sudo dnf install rsyslog
```

> *Verification Tip: Confirm Rsyslog is installed successfully*

1.4 Start and Enable Rsyslog Service

```
sudo systemctl enable rsyslog
sudo systemctl start rsyslog
```

1.5 Check Rsyslog Status

```
sudo systemctl status rsyslog
```

> *Expected Result*: Service should be in an active state

Step 2: Rsyslog Server and Client Configuration

The following steps outline how to forward system logs to a remote server using either TCP or UDP ports. You can choose to use either TCP or UDP, but if both are enabled, ensure that each protocol uses a different port.

2.1 Edit Rsyslog Configuration. Open using a text editor such as "vi" or "nano".

```
vi /etc/rsyslog.conf
```

2.2 Enable UDP or TCP Modules. This should be done on the Client machine only.

- For **UDP**, locate and uncomment the following lines by removing the `#` symbol. The default port is 514, but you can change it if necessary.

```
$Modload imudp
$UDPServerRun 514
```

- For **TCP**, locate and uncomment the following lines by removing the `#` symbol. The default port is 10514, but you can change it if necessary.

```
$Modload imtcp
$inputTCPServerRun 10514
```

2.3 Configure Log Template
Add the following line to define log storage:

```
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~
```

2.4 **On Server**
Add content below at the end of the file */etc/rsyslog.conf.*
This will configure the log forwarding to the remote host. Please update the "target", "port" and "tcp" appropriately.

```
*.* action(type="omfwd"
queue.type="LinkedList"
action.resumeRetryCount="-1"
queue.size="10000"
queue.saveonshutdown="on"
target="10.43.138.1" Port="10514" Protocol="tcp")
```

queue.type enables a LinkedList in-memory queue, queue_type can be *direct*, *linkedlist* or *fixedarray* (which are in-memory queues), or disk.
enabled **queue.saveonshutdown** saves in-memory data if rsyslog shuts down,
action.resumeRetryCount= “-1” setting prevents rsyslog from dropping messages when retrying to connect if server is not responding,
queue.size where size represents the specified size of disk queue part. The defined size limit is not restrictive, rsyslog always writes one complete queue entry, even if it violates the size limit.
target is the IP Address of the remote machine
Port is the port of the remote machine
Protocol is the protocol to be used. Values can be udp or tcp.

2.5 Add port in the firewall rules

On client side
Add the provided port to the firewall

```
iptables -A INPUT -p tcp --dport 10514  -j ACCEPT
```

Next open the port using nc

```
nc -l -p 10514 -4
```

2.6 Apply Server Configuration

```
systemctl restart rsyslog
```

2.7 Verify Log Directory
Type : ls -1
Expected Result:
Should see a directory with the client's hostname
Contains files like `rsyslogd.log` and `systemd.log`

Troubleshooting Tips
Ensure firewall settings allow log forwarding
Verify network connectivity between client and server
Check Rsyslog service status if logs aren't forwarding

Security Considerations
- Configure firewall rules appropriately
- Use encrypted log transmission when possible
- Regularly review and rotate logs

Common Issues
1. Port Blocking: Ensure port 514 is open
2. Permission Errors Verify root/sudo access

3. Network Connectivity: Check server IP and network settings

Conclusion
By following these steps, you should have successfully configured Rsyslog for log forwarding between a client and a remote server.

Note: Always test in a controlled environment first and adapt instructions to your specific system configuration.

Revision #14
Created 17 December 2024 13:40:52 by CyTech Admin
Updated 18 December 2024 08:41:02 by Aldion Pueblos