For more information on the Kernel Side-Channel Attack using Speculative Store Bypass - CVE-2018-3639, please refer to this Vulnerability Page (https://red.ht/ssbd).

How to configure remote logging with rsyslog

SOLUTION VERIFIED - Updated August 19 2016 at 8:41 PM - English ()

Environment

- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- rsyslog

Issue

- How to configure remote logging with `rsyslog`
- How to configure system to accept remote log messages in Red Hat Enterprise Linux
- How to send remote log messages to another server with `rsyslog`
- How to configure RHEV Hypervisor for remote logging using 'rsyslog'

Resolution

In RHEL-6 rsyslog is default logging daemon, In RHEL-5 rsyslog is available but not installed by default.

- Install rsyslog

```
# yum install rsyslog
```

- To configure `rsyslog` using TCP:

1. Configure the remote server to accept remote log messages using TCP.

Uncomment the following lines in the **MODULES** section of `/etc/rsyslog.conf` , In RHEL-5 you have to add the lines to beginning of `/etc/rsyslog.conf` :


```
$ModLoad imtcp
$InputTCPServerRun 514
```

Restart rsyslog.

```
[root@server1 ~]# service rsyslog restart
```

In RHEL-5 first stop the default `syslog` deamon and after that restart the `rsyslog` .

```
[root@server1 ~]# service syslog stop
[root@server1 ~]# service rsyslog restart
```

2. Configure the `rsyslog` to send `rsyslog` events to another server using TCP.

   Add the following line to the **RULES** section of `/etc/rsyslog.conf` or in RHEL-5 at the end of the `/etc/rsyslog.conf` :

```
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @remote-host:514
*.*         @@10.10.10.1:514
```

   You can also specify the severity to send, for example info messages:

```
*.info      @@10.10.10.1:514
```

   Restart rsyslog.

```
[root@server2 ~]# service rsyslog restart
```

   In RHEL-5 first stop the default `syslog` deamon and after that restart the `rsyslog` .

```
[root@server2 ~]# service syslog stop
[root@server2 ~]# service rsyslog restart
```

- Configure the remote server to accept remote log messages using UDP.

  1. Configure the server to accept remote log messages using UDP.

Uncomment the following lines in the **MODULES** section of `/etc/rsyslog.conf` , In RHEL-5 you have to add the lines to beginning of `/etc/rsyslog.conf` :

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

Restart rsyslog.

```
[root@server1 ~]# service rsyslog restart
```

In RHEL-5 first stop the default `syslog` deamon and after that restart the `rsyslog` .

```
[root@server1 ~]# service syslog stop
[root@server1 ~]# service rsyslog restart
```

2. Configure the `rsyslog` server to send `rsyslog` events to another server using UDP.

   Add the following line to the RULES section of `/etc/rsyslog.conf` or in RHEL-5 at the end of the `/etc/rsyslog.conf` :

   ```
   # remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
   #*.* @remote-host:514
   *.*         @10.10.10.1:514
   ```

   You can also specify the severity to send, for example info messages:

   ```
   *.info      @10.10.10.1:514
   ```

   Restart rsyslog.

   ```
   [root@server2 ~]# service rsyslog restart
   ```

   In RHEL-5 first stop the default `syslog` deamon and after that restart the `rsyslog` .

   ```
   [root@server2 ~]# service syslog stop
   [root@server2 ~]# service rsyslog restart
   ```

- Test the configuration:

  On server2 (`rsyslog` sending out the messages):

```
[root@server2 ~]# logger Test from system
[root@server2 ~]# tail /var/log/messages
Dec 25 00:00:01 server2 root: Test from system
```

On server1 (`rsyslog` receiving the messages)

```
[root@server1 ~]# tail /var/log/messages
Dec 25 00:00:01 server2 root: Test from system
```

- While not specifically rsyslog related, additional selinux changes are required if you would like to run rsyslog on a non-standard port. this additional configuration is not necessary under normal usage. In place of 'tcp 514', use the alternate protocol and port you wish to use.

```
# semanage port -l| grep syslog
syslogd_port_t                 udp      514
# semanage port -a -t syslogd_port_t -p tcp 514
```

Note: when configuring remote logging, please make sure to also review and configure action queues (https://access.redhat.com/solutions/330693) in order to avoid potential issues when the remote rsyslog server is unreachable.

Product(s) **Red Hat Enterprise Linux (/taxonomy/products/red-hat-enterprise-linux)**

Component **logrotate (/components/logrotate)** **rsyslog (/components/rsyslog)**

Category **Configure (/category/configure)**

Tags **rhel (/tags/rhel)** **rhel_5 (/tags/rhel_5)** **rhel_6 (/tags/rhel_6)** **rhel_7 (/taxonomy/tags/rhel7)** **syslog (/tags/syslog)**

This solution is part of Red Hat's fast-track publication program, providing a huge library of solutions that Red Hat engineers have created while supporting our customers. To give you the knowledge you need the instant it becomes available, these articles may be presented in a raw and unedited form.
