Windows Event Forwarding to Linux server using Nxlog

Introduction

Windows Event Forwarding (WEF) allows the collection of event logs from multiple Windows machines and their forwarding to a centralized server. Using Nxlog, you can send these logs to a Linux server for storage and analysis. This documentation provides a step-by-step guide to set up Windows Event Forwarding using Nxlog to send logs to a Linux server.

Prerequisites

- **Windows Server or Workstation**: The machine that will send logs.
- **Linux Server**: The machine that will receive logs.
- **Nxlog**: Download the latest version of Nxlog for Windows from Nxlog's official website.
- **Network Connectivity**: Ensure both machines can communicate over the network.
- **Rsyslog:** Download the latest version of Rsyslog for Linux server or workstation.

Installing Nxlog on Windows

1. **Download Nxlog**:
   - Obtain the Nxlog Community Edition installer from the official website.
2. **Install Nxlog**:
   - Run the installer and follow the prompts to complete the installation.
3. **Start Nxlog Service**:
   - Start the Nxlog service using the Services management console or command line: **net start nxlog**

Configuring Nxlog on Windows

1. **Open Configuration File**:
   - Edit the Nxlog configuration file located at `C:\Program Files\nxlog\conf\nxlog.conf`.
2. **Configure File**:
   - Add the following lines to capture Windows Event Logs and send the logs :

```
# Input Module
<Input eventlog>
    Module im_msvistalog
    ReadFromLast True
    <QueryXML>
<QueryList>
<Query Id='1'>
<Select Path='Application'>*</Select>
<Select Path='Security'>*</Select>
<Select Path='System'>*</Select>
</Query>
</QueryList>
     </QueryXML>
</Input>

# Output Module
<Output out>
    Module om_udp
    Host 192.168.20.24
    Port 514
   # Exec $raw_event = "<" + $syslog_severity + ">" + $time + " " + $hostname +
" " + $procname + ": " + $raw_event;
    Exec parse_syslog_ietf();
</Output>

# Route
<Route r>
    Path eventlog => out
</Route>

# Include any other necessary modules/extensions
<Extension _syslog>
    Module      xm_syslog
</Extension>
```

Installing Rsyslog on Linux

- **Install Rsyslog**:
  - For Ubuntu, run:
    sudo apt update sudo apt install rsyslog

- **Enable Rsyslog**:
  - Ensure Rsyslog is enabled and started:
    sudo systemctl enable rsyslog sudo systemctl start rsyslog

Configuring Rsyslog on Linux

1. **Open Configuration File**:
   - Edit /etc/rsyslog.conf or create a new config file in /etc/rsyslog.d/.
2. **Configure Rsyslog to Listen for UDP**:**module(load="imudp") # Load UDP listener input(type="imudp" port="514")**
3. **Define Output File**:
   - Specify where to store the incoming logs:
   ***.* /var/log/windows_events.log**
4. **Save and Exit**:
   - Save the configuration file and restart Rsyslog:
     sudo systemctl restart rsyslog

Firewall Configuration

Windows Firewall

1. **Open Windows Defender Firewall**:
   - Go to **Control Panel** > **System and Security** > **Windows Defender Firewall**.
2. **Allow Port 514**:
   - In the left pane, click **Advanced settings**.
   - Select **Inbound Rules** and click on **New Rule**.
   - Choose **Port**, then click **Next**.
   - Select **UDP** and enter **514** in the Specific local ports field.
   - Allow the connection and complete the rule setup.

Firewalld Configuration on Linux

1. **Open Port 514 for UDP**:
   sudo firewall-cmd --permanent --add-port=514/udp
2. **Reload Firewalld**:
   sudo firewall-cmd --reload
3. **Verify Open Ports**:
   sudo firewall-cmd --list-all

Verifying Event Forwarding

1. **Check Nxlog Status on Windows**:
   nxlog -v
2. **Monitor Logs on Linux**:
   - Use the following command to view the log file:
   tail -f /var/log/windows_events.log
3. **Review Rsyslog Logs**:

- If issues arise, check Rsyslog logs located at **/var/log/syslog** or **/var/log/messages.**

Revision #1
Created 22 October 2024 06:49:45
Updated 22 October 2024 07:16:22