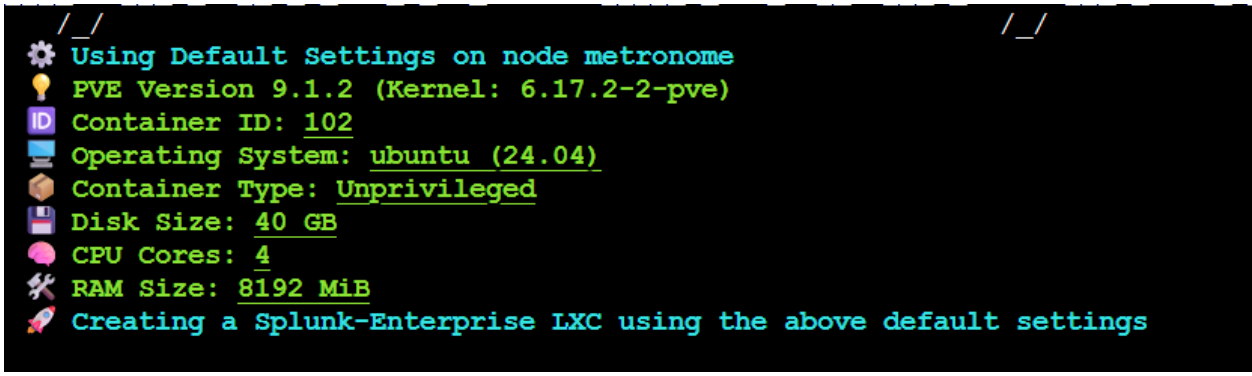
Proxmox Guide – Splunk

Pre-requisites

- Proxmox node
- Splunk account

Splunk Setup

1. In the node, select "Shell" and run the following script:
    a. bash -c "$(curl -fsSL https://raw.githubusercontent.com/community-scripts/ProxmoxVE/main/ct/splunk-enterprise.sh)"
    b. Script is from: https://community-scripts.github.io/ProxmoxVE/scripts?id=splunk-enterprise
    c. Default setup information:



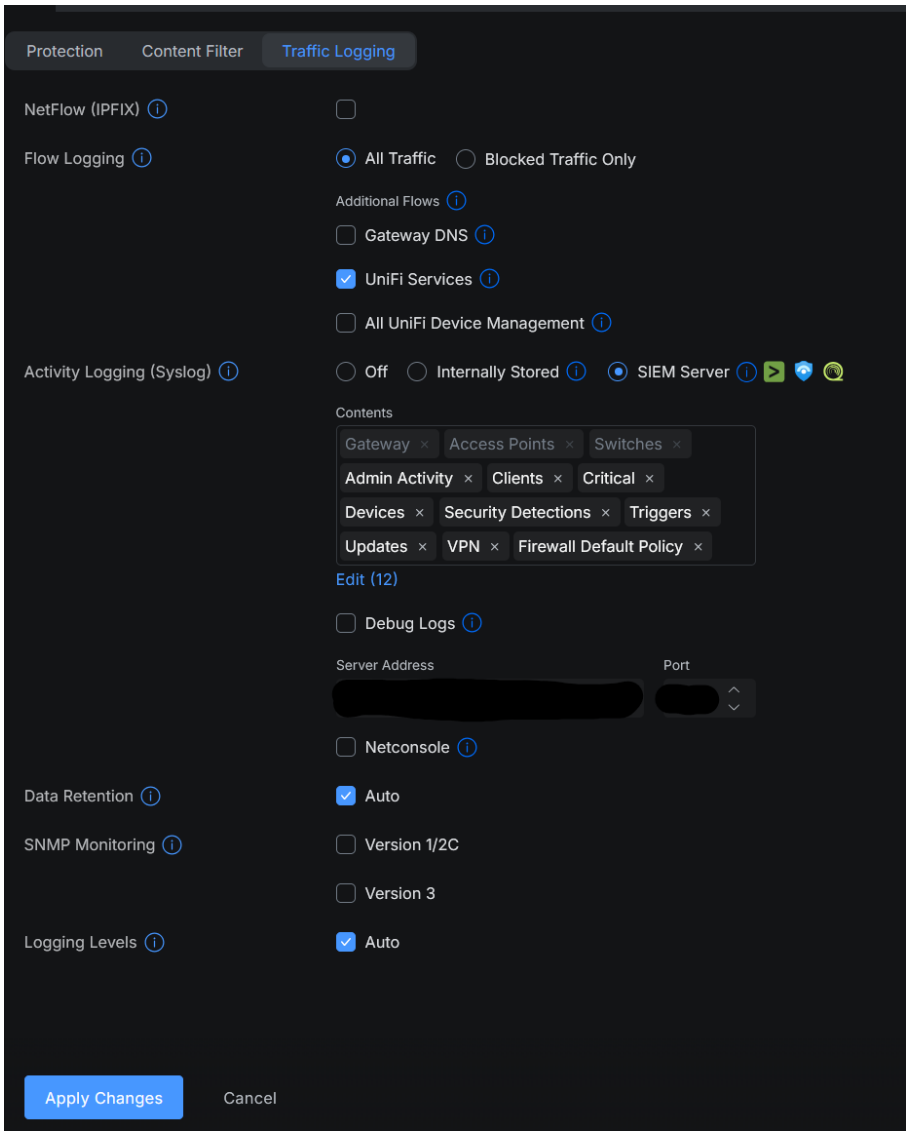
2. Once completed, you'll be presented with an IP and port to connect to.
3. For the first time login credentials:
    a. Open the Splunk container in Proxmox and go into the console
    b. By default you should already be in the directory containing the splunk.creds file
    c.

```
root@splunk-enterprise:~# ls
splunk.creds
root@splunk-enterprise:~# cat splunk.creds
Splunk-Credentials
```

    d. If you cannot locate the splunk.creds file, use a command like readlink to locate the file
    e.

```
root@splunk-enterprise:~# readlink -f splunk.creds
/root/splunk.creds
```

Connecting Splunk to Unifi Router

1. Login to your router
2. Navigate to Settings>CyberSecure>Traffic Logging
3. Select SIEM Server next to Active Logging
4. Enter in your Splunk server's IP and port, and select what content you want sent to Splunk
    a. 

5. Apply your changes