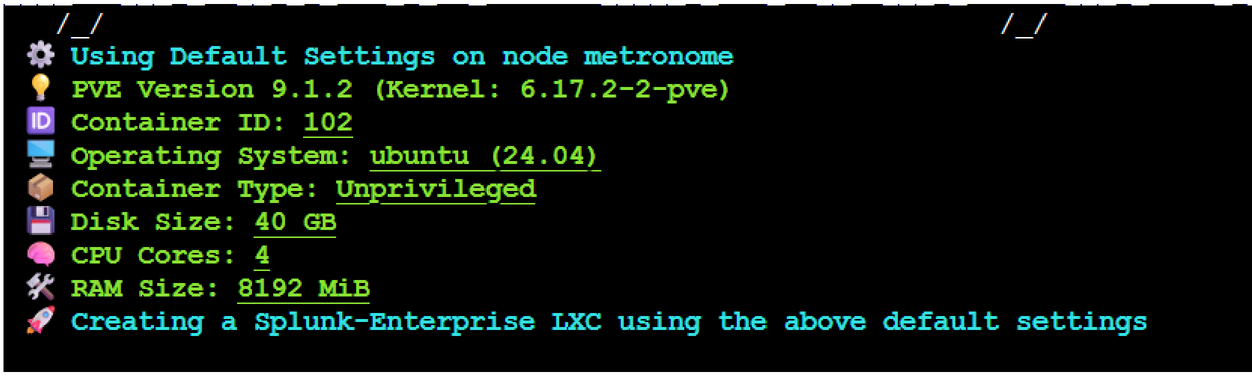
Proxmox Guide – Splunk

Pre-requisites

- Proxmox node
- Splunk account

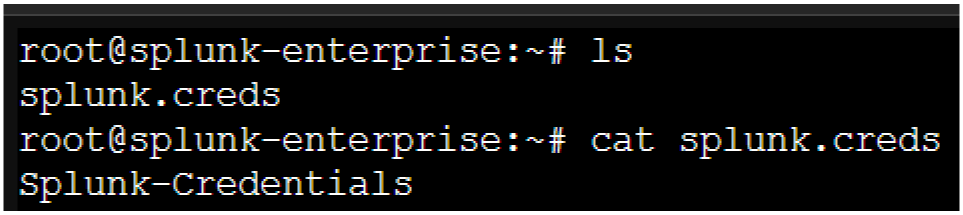
Initial Setup

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:



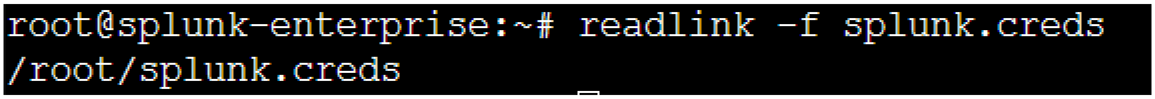
```
  /_/                                                    /_/
⚙️  Using Default Settings on node metronome
💡  PVE Version 9.1.2 (Kernel: 6.17.2-2-pve)
🆔  Container ID: 102
🖥️  Operating System: ubuntu (24.04)
📦  Container Type: Unprivileged
💾  Disk Size: 40 GB
🧠  CPU Cores: 4
🛠️  RAM Size: 8192 MiB
🚀  Creating a Splunk-Enterprise LXC using the above default settings
```

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.



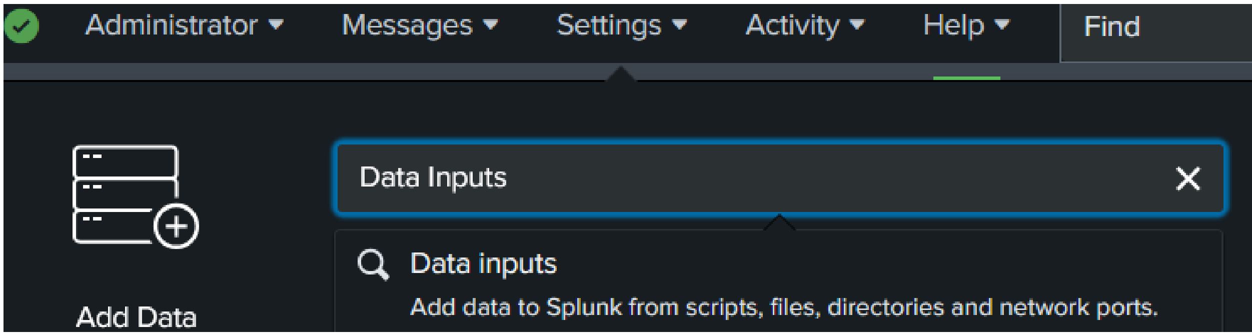
```
root@splunk-enterprise:~# ls
splunk.creds
root@splunk-enterprise:~# cat splunk.creds
Splunk-Credentials
```

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

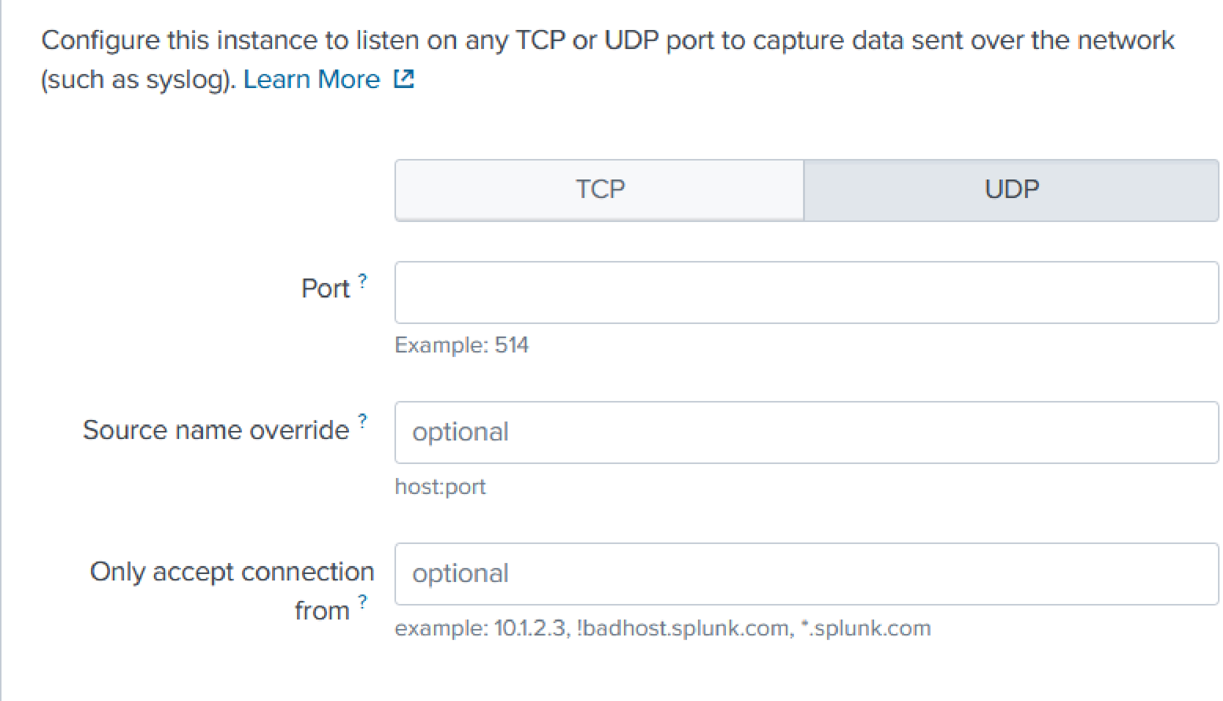


```
root@splunk-enterprise:~# readlink -f splunk.creds
/root/splunk.creds
```

Splunk Connection

1. Login to your Splunk server, go to settings, then Data Inputs
   a. 

   Data Inputs ✕

   Data inputs
   Add data to Splunk from scripts, files, directories and network ports.
2. Select UDP then New Local UDP
3. Follow the setup wizard to connect your UDM SE
   a. 

   Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More

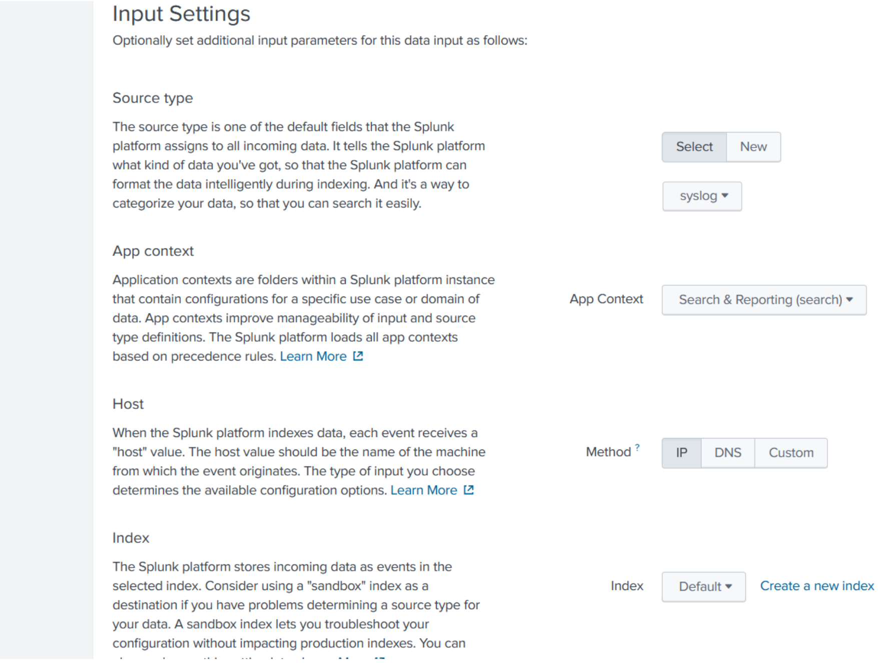
   TCP | UDP

   Port ?
   Example: 514

   Source name override ? optional
   host:port

   Only accept connection from ? optional
   example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

   b. Enter a port number such as 514
   c. Name your source
4. On the Input Settings
   a. Use the syslog for Source Type
   b. Use Search & Reporting for App Context
   c. Use whichever you prefer for Host
   d. Under Index you should setup a custom index, but you can use default.

e. 

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

syslog ▾

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

App Context: Search & Reporting (search) ▾

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

Method ?: IP | DNS | Custom

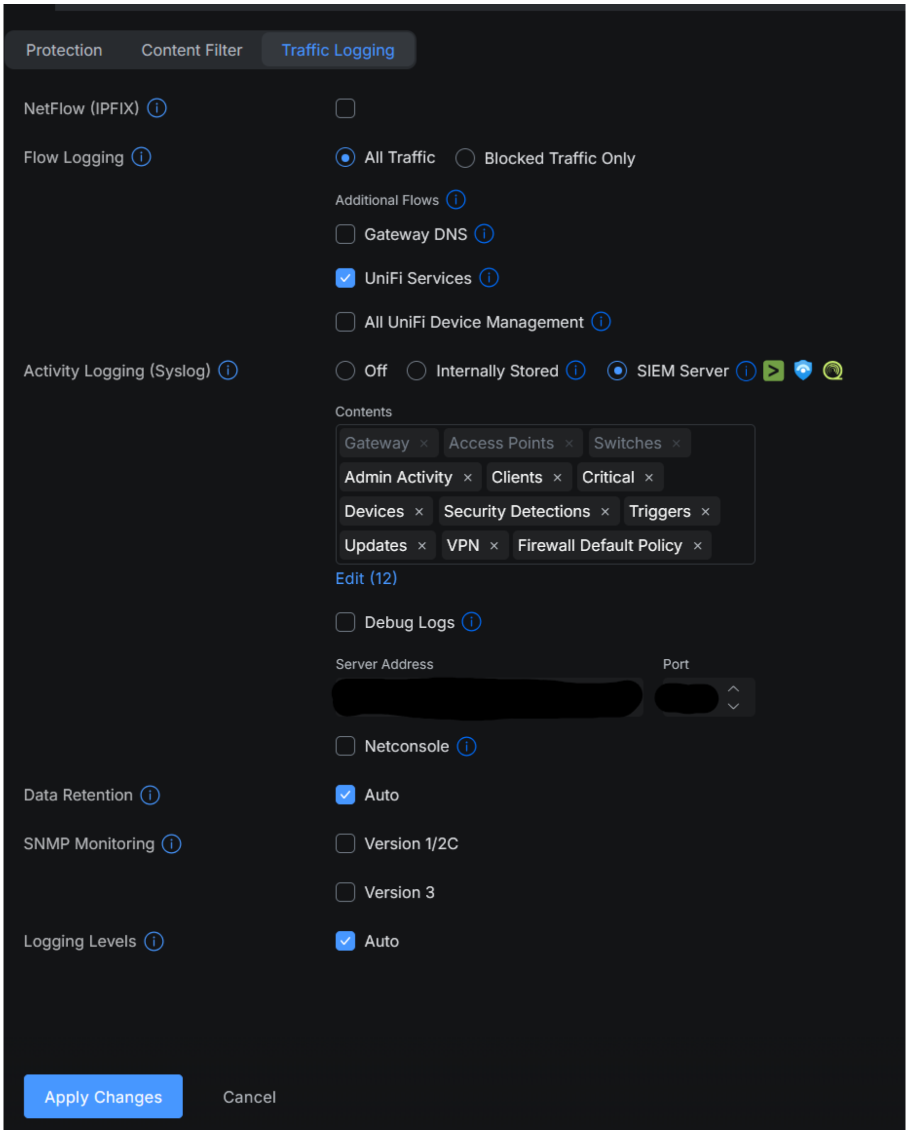
Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can

Index: Default ▾

5. Review your options and confirm

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 set during the Splunk Connection section of this guide. Then select what content you want sent to Splunk
   a. 

      Protection Content Filter Traffic Logging

      NetFlow (IPFIX) ⓘ □

      Flow Logging ⓘ ● All Traffic ○ Blocked Traffic Only

      Additional Flows ⓘ

      □ Gateway DNS ⓘ

      ☑ UniFi Services ⓘ

      □ All UniFi Device Management ⓘ

      Activity Logging (Syslog) ⓘ ○ Off ○ Internally Stored ⓘ ● SIEM Server ⓘ

      Contents

      Gateway × Access Points × Switches ×
      Admin Activity × Clients × Critical ×
      Devices × Security Detections × Triggers ×
      Updates × VPN × Firewall Default Policy ×

      Edit (12)

      □ Debug Logs ⓘ

      Server Address [redacted] Port [redacted]

      □ Netconsole ⓘ

      Data Retention ⓘ ☑ Auto

      SNMP Monitoring ⓘ □ Version 1/2C

      □ Version 3

      Logging Levels ⓘ ☑ Auto

      Apply Changes Cancel
5. Apply your changes

After a few minutes you should start to see logs flowing into your Splunk dashboard.