**Installation Guide for Grafana Loki**

**Overview**

Grafana Loki is a log aggregation system inspired by Prometheus. It's designed to be cost-effective and easy to operate because it does not index the contents of the logs, but rather a set of labels for each log stream.

**Prerequisites**

* A machine with either Windows, Linux, or macOS.
* Basic command-line interface (CLI) knowledge.
* Docker installed on your machine (for ease of setup).

**Step 1: Install Docker**

* **Windows & macOS**: Download and install Docker Desktop from Docker Hub.
* **Linux**: Use your distribution's package manager. For example, on Ubuntu, you would use:

bash

* sudo apt-get update
* sudo apt-get install docker-ce docker-ce-cli containerd.io

**Step 2: Run Loki and Grafana with Docker**

1. **Pull the Docker Compose File**:
   * Create a new directory for your Loki setup.
   * Download the official docker-compose.yml for Loki from the [Grafana Loki GitHub repository](https://github.com/grafana/loki/blob/main/production/docker-compose.yml) (<https://github.com/grafana/loki>) to the directory you created. You can do this by visiting the URL, copying the content to a new file named docker-compose.yml in your directory.
2. **Run Docker Compose**:
   * Open a terminal or command prompt.
   * Navigate to the directory containing your docker-compose.yml.
   * Run the following command to start Loki and Grafana:

bash

* + docker-compose up
  + This command downloads the necessary Docker images for Loki and Grafana and starts them.

**Step 3: Access Grafana**

* Once the Docker containers are running, open a web browser and go to http://localhost:3000.
* Log in to Grafana using the default credentials (admin for both username and password).
* You will be prompted to change the password. Choose a new password and proceed.

**Step 4: Add Loki as a Data Source in Grafana**

1. In the Grafana dashboard, click on the gear icon on the left sidebar to go to **Configuration > Data Sources**.
2. Click on **Add data source**, and choose **Loki**.
3. Set the URL to http://loki:3100, which is the Loki service running in your Docker setup.
4. Click **Save & Test** to ensure Grafana can communicate with Loki.

**Step 5: Explore Logs**

* To start exploring logs, click on the compass icon on the left sidebar to go to **Explore**.
* Choose **Loki** from the data source selector.
* You can now run queries to explore your logs.

**Step 6: Basic Troubleshooting**

* **If Grafana or Loki fails to start**, check the Docker logs using docker-compose logs for any error messages.
* **If you can't access Grafana**, ensure Docker is running and that there are no firewall rules blocking access to port 3000.

**Notes**

* This guide uses Docker for simplicity and compatibility across different operating systems. Running Loki and Grafana directly on your machine is possible but involves more steps.
* This setup is intended for learning and experimentation. For production environments, consider additional security measures and configurations.

Congratulations! You now have a basic log monitoring setup with Grafana Loki. This guide is designed to help cybersecurity beginners get hands-on experience with log aggregation and monitoring.

**1. Universal Hardening Guide**

**Step-by-Step Actions:**

**1. Update & Patch**

* **Command**: Different based on OS; generally, use the system's update tool (e.g., for Linux: sudo apt-get update && sudo apt-get upgrade).
* **Purpose**: Ensures all software and the OS are up to date, patching known vulnerabilities.

**2. Password Policy Enforcement**

* **Finding Users/Groups**:
  + Linux: cat /etc/passwd (for users), cat /etc/group (for groups).
  + Windows: net user (lists users), net localgroup (lists groups).
* **Setting a Secure Policy**:
  + Use complex passwords (mix of uppercase, lowercase, numbers, symbols, 12+ characters).
  + Change default passwords immediately.
  + **Command**:
    - Linux: passwd [username] to change passwords.
    - Windows: net user [username] [new password] to change passwords.

**3. Firewall Configuration**

* **Enable Firewall**:
  + Linux: sudo ufw enable.
  + Windows: Search for "Windows Defender Firewall" and turn it on.
* **Configure Rules**:
  + Deny all inbound connections by default.
  + Allow specific necessary inbound/outbound connections.

**After These Steps**:

* **Monitoring**: Watch for repeated failed login attempts, unexpected software installations, or unusual network traffic.
* **Tools**: Use system logs (Linux: /var/log/, Windows: Event Viewer).

**2. Router and Printer Hardening**

**Identifying Devices on the Network**:

* Use a network scanning tool like nmap (if pre-installed) to identify devices.

**Steps for Hardening**:

* **Change Default Passwords**: Access device settings via its IP address in a browser.
* **Update Firmware**: Look for firmware updates in the device's web admin panel.
* **Disable Unused Services**: In device settings, turn off any features not in use (e.g., remote management).

**3. Windows Server Hardening**

**Update and Patch**:

* Access via Control Panel > System and Security > Windows Update.

**Configure User Rights/Access Control**:

* Use Group Policy Editor (gpedit.msc).
* Minimize administrative privileges; only necessary personnel should have admin access.

**Enable and Configure Windows Firewall**:

* Access via Control Panel > System and Security > Windows Defender Firewall.
* Use Advanced settings to fine-tune rules.

**4. High-Priority Actions**

**Firewall/Network**:

* Initially block all inbound traffic except essential services.
* Use the firewall's settings to configure (as detailed in the universal guide).

**Active Directory (AD) Hardening**:

* Enforce strong password policies through Group Policy.
* Limit administrative privileges; use role-based access control.

**5. Database Server & Webserver Hardening**

**Database Server**:

* **Change Default Passwords & Enforce Strong Authentication**.
* **Limit Connections**: Only allow connections from specific, necessary services.
* **Protect Against SQL Injection**: Use prepared statements and parameterized queries.

**Webserver**:

* **Use HTTPS**: Check your web server documentation for SSL/TLS setup instructions.
* **Disable Directory Listing**: Look for Options -Indexes in Apache or directoryBrowse setting in IIS.
* **Update Software**: Regularly check and apply updates for your web server and any platforms (e.g., CMS) running on it.

**Memo to Employees: Post-Network Maintenance Notification**

**Subject:** Network Maintenance Update and Password Reset

Dear Team,

We are pleased to announce that the network maintenance has been successfully completed, and full system functionality has been restored. We want to extend our sincerest thanks for your patience and understanding during this necessary downtime.

As part of our security enhancements, we have reset certain parts of the system. You will be prompted to change your password upon your next login. This is a precautionary measure to ensure the continued security of our network and your data.

Should you encounter any issues or require assistance, please feel free to reach out to the IT/Security team.

Once again, thank you for your cooperation and understanding as we work together to maintain a secure and efficient working environment.

Warm regards,  
[Your Name]  
[Your Position]  
IT/Security Team

**Expanded System Discovery and Hardening Information Sheet**

**Enhanced System Information**

**1. Network Role and Relationships**

* **Simple Discovery Direction**: Use ping to check connectivity to known devices or arp -a to list all devices your system has communicated with.
* **Record Here**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**2. CPU and System Resources**

* **Windows (PowerShell)**: Get-Process | Sort CPU -Descending | Select -First 5.
* **Linux (top command)**: Use top to view active processes. Press Shift+M to sort by memory usage, P to sort by CPU usage. Look for %CPU and %MEM columns for resource usage.
* **Record Here**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3. Log Captures Upon Start for Baseline**

* **Windows**: Use Get-EventLog -LogName System -Newest 50 in PowerShell to view recent system logs.
* **Linux**: Use tail -n 50 /var/log/syslog or /var/log/dmesg for system logs.
* **Record Here**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Additional Vital Information**

**4. System Name**

* **Command**:
  + Windows: hostname.
  + Linux: hostname or uname -n.
* **Record Here**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**5. Operating System and Version**

* **Command**:
  + Windows: systeminfo | findstr /B /C:"OS Name" /C:"OS Version".
  + Linux: lsb\_release -a or cat /etc/\*release.
* **Record Here**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**6. MAC Address**

* **Command**:
  + Windows: getmac.
  + Linux: ip link or ifconfig -a.
* **Record Here**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Managing Ports**

**Closing a Port or Redirecting Traffic**

* **Closing a Port**:
  + **Windows**: Use Windows Firewall settings. For command line, New-NetFirewallRule -DisplayName "BlockPortXXXX" -Direction Inbound -LocalPort XXXX -Protocol TCP -Action Block in PowerShell.
  + **Linux**: Use iptables, e.g., sudo iptables -A INPUT -p tcp --dport XXXX -j DROP to block incoming connections on port XXXX.
* **Redirecting Traffic**:
  + **Linux**: Use iptables for redirection, e.g., sudo iptables -t nat -A PREROUTING -p tcp --dport [original\_port] -j REDIRECT --to-port [new\_port].
  + Windows lacks a built-in command for port redirection but can be managed through Routing and Remote Access Service (RRAS) for more complex networking setups.
* **Key Ports, Protocols, and Security Ranking**

| **Port Number** | **Protocol/Standard Use** | **Security Ranking** | **Open/Closed** |
| --- | --- | --- | --- |
| 22 | SSH (Secure Shell) | Medium | [ ] Open [ ] Closed |
|  |  |  |  |
| 23 | Telnet (Unsecure Shell) | Low | [ ] Open [ ] Closed |
|  |  |  |  |
| 25 | SMTP (Email Sending) | Medium | [ ] Open [ ] Closed |
|  |  |  |  |
| 53 | DNS (Domain Name System) | Medium | [ ] Open [ ] Closed |
|  |  |  |  |
| 80 | HTTP (Unsecure Web Traffic) | Low | [ ] Open [ ] Closed |
|  |  |  |  |
| 443 | HTTPS (Secure Web Traffic) | High | [ ] Open [ ] Closed |
|  |  |  |  |
| 445 | SMB (Windows File Sharing) | Low | [ ] Open [ ] Closed |
|  |  |  |  |
| 3389 | RDP (Remote Desktop Protocol) | Medium | [ ] Open [ ] Closed |

**Memo to Employees: Pre-Network Shutdown Notification**

**Subject:** Upcoming Network Maintenance and Temporary Downtime

Dear Team,

We hope this message finds you well. We want to inform you of an upcoming necessary network shutdown to resolve a system error that has been identified. This action is scheduled to ensure the security and reliability of our IT infrastructure and will take place [insert date and time here]. We anticipate the downtime will be brief and are working diligently to minimize the impact on your work.

We understand the inconvenience this may cause and respect the importance of your roles and responsibilities. Our team is committed to restoring full network functionality as quickly as possible.

Should you have any questions or require assistance during this period, please do not hesitate to contact the IT/Security team.

Thank you for your understanding and cooperation.

Best Regards,  
[Your Name]  
[Your Position]  
IT/Security Team

**Memo to the C-Suite: Explanation of Network Shutdown**

**Subject:** Recent Network Maintenance: A Necessary Precaution

Dear [C-Suite Executive's Name],

I hope this message finds you well. I wish to provide you with an overview and rationale for the recent network shutdown that took place [insert date and time here], which resulted in a temporary pause of our systems for approximately one hour.

Our team identified several serious vulnerabilities within our network that presented potential risks for a cyber-attack. These vulnerabilities, if exploited, could have compromised the integrity and security of our business assets, including sensitive information related to our customers, employees, and the company's reputation.

To illustrate, consider the scenario of a market or deli manager discovering a power outage that may have affected the safety of perishable goods in the cooler. Despite the cost and inconvenience, prioritizing health and safety by discarding potentially compromised products is paramount. Similarly, we took immediate action to address and mitigate these vulnerabilities to avoid potential damages that, while not immediately visible, could have had long-lasting impacts.

This decision, while not taken lightly, was necessary to protect the integrity and security of our business. The successful completion of this maintenance has significantly reduced the risk of a cyber-attack. Moving forward, we are implementing additional monitoring systems to ensure that we can proactively identify and address such issues more efficiently.

We understand the significance of this decision and its impact on operations. However, just as the deli manager prioritizes the health and safety of the community, we must prioritize the security of our digital environment.

Thank you for your understanding and support as we continue to ensure the safety and reliability of our IT infrastructure.

Best regards,  
[Your Name]  
[Your Position]  
IT/Security Team

Sure thing! Let's expand on the specifics for handling an email server and domain at the administrative level, detail an emergency network shutdown procedure, and outline how to identify connected devices and access their admin interfaces.

**Email Server and Domain Administration**

**Email Server:**

* **Purpose**: Handles sending, receiving, and storing emails for your domain.
* **Key Information to Gather**:
  + **Server Type** (e.g., Exchange, Postfix): Identify the software or service used.
  + **Configuration Files**: Location varies by software; commonly /etc/postfix/main.cf for Postfix.
  + **Admin Interface Access**: Often accessible via web interface or specific management tools.
  + **Record Here**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Email Domain:**

* **Purpose**: The domain part of an email address (e.g., @example.com) that routes emails to the correct server.
* **Key Information to Gather**:
  + **DNS MX Records**: Use nslookup -query=MX yourdomain.com to find mail exchange records.
  + **SPF, DKIM, and DMARC Records**: Check your domain's DNS settings for these email authentication methods.
  + **Record Here**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Emergency Network Shutdown and Purge**

**Closing Off the Network (Emergency Shutdown):**

* **Windows**: Use PowerShell or Windows Firewall with Advanced Security to create a rule blocking all inbound and outbound connections, e.g., New-NetFirewallRule -Name "BlockAll" -Direction Inbound -Action Block -Profile Any.
* **Linux**: Use iptables to block all traffic, e.g., sudo iptables -P INPUT DROP; sudo iptables -P FORWARD DROP; sudo iptables -P OUTPUT DROP.

**Purging Machines/Addresses from the Network:** While there's no universal "reset" button for purging all machines from a network via the firewall, you can:

* **Reassign IP Addresses**: Change the IP range of the network to effectively "disconnect" unauthorized devices.
* **MAC Address Filtering**: Implement a whitelist of allowed MAC addresses on your network devices.
* **Network Reconfiguration**: In extreme cases, reconfiguring network settings (including SSIDs for wireless networks) can help remove unwanted devices.