Modern Linux Logging—Chopping through Data like a pro

- A Guide To Systemd Journal Management

Andrew Denner
1/15/2024
Central Iowa Linux Users Group

Insert Standard intro here

- Andrew Denner
  - https://denner.co
  - President of CIALUG
  - Senior Scientific Software Developer
  - All the standard social medias:
    - https://denner.co/social/

Introduction

Why we log

The data forest

- Every application tells a story
- Logs are our trail markers through the code forest
  - System health monitoring
  - Debugging and troubleshooting
  - Security and compliance

Journey Through the Logs

- Traditional Logging vs Journal
- Why systemd Journal?
  - Structured logging
  - Built-in indexing
  - Native system integration

The Core Components

The Tools of the trade

- journalctl
- systemd-journal
- journal API

Basic operations

Reading Logs:

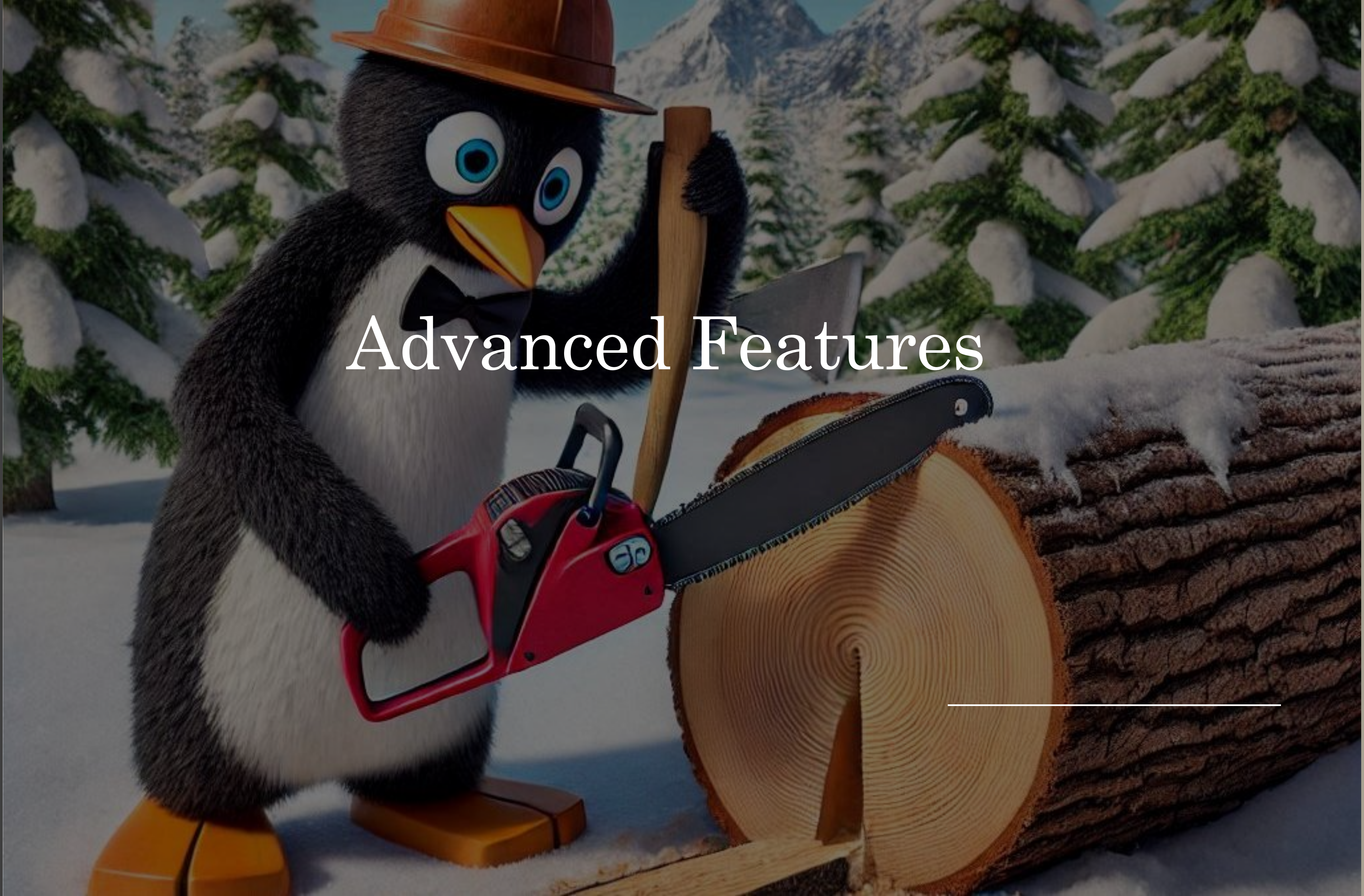
Filtering

Following

Time-based queries

Log Structure

- Metadata Fields
- Priority Levels
- Context Information



Advanced Features

Precision Logging

- - Structured Data
- - Custom Fields
- - Correlation IDs

Remote Logging

- - Network Transport
- - Log Aggregation
- - Central Management

Performance Optimization

- Batch Processing
- - Resource Management
- - Storage Optimization

Security

Securing the forest

- Access Controls
- - Encryption
- - Audit Trails

Data Protection

- - Sensitive Data Handling
- - Masking
- - Encryption

Compliance & Auditing

- - Regulatory Requirements
- - Audit Logging
- - Retention Policies

Integration Patterns

Connected Forests

- Explore the integration of microservices for efficient logging.
- Utilize cloud services to enhance data accessibility.
- Implement event-driven systems for real-time log processing.

Send remote logs via systemd

- # Install the required package
- sudo apt install systemd-journal-remote   # Debian/Ubuntu
- # or
- sudo dnf install systemd-journal-remote   # RHEL/Fedora
- # Create/edit the config
- sudo vim /etc/systemd/journal-upload.conf

```
[Upload]
URL=https://your-remote-server:19532
ServerKeyFile=/etc/ssl/private/journal-upload.pem
ServerCertificateFile=/etc/ssl/certs/journal-upload.pem
TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Cont.

```
[Remote]

Listen=19532

ServerKeyFile=/etc/ssl/private/journal-remote.pem

ServerCertificateFile=/etc/ssl/certs/journal-remote.pem
```

```
openssl req -x509 -nodes -newkey rsa:4096 \

 -keyout journal-remote.pem \

  -out journal-remote.pem \

  -days 365 \

  -subj "/CN=journal-remote“

# On sender

sudo systemctl enable --now systemd-journal-upload



# On receiver

sudo systemctl enable --now systemd-journal-remote
```

Modern Logging Architecture

- Distributed Systems
- Container Integration
- Cloud-Native Logging

Metrics & Monitoring

- **Performance Metrics**
- **Health Monitoring**

Best practices

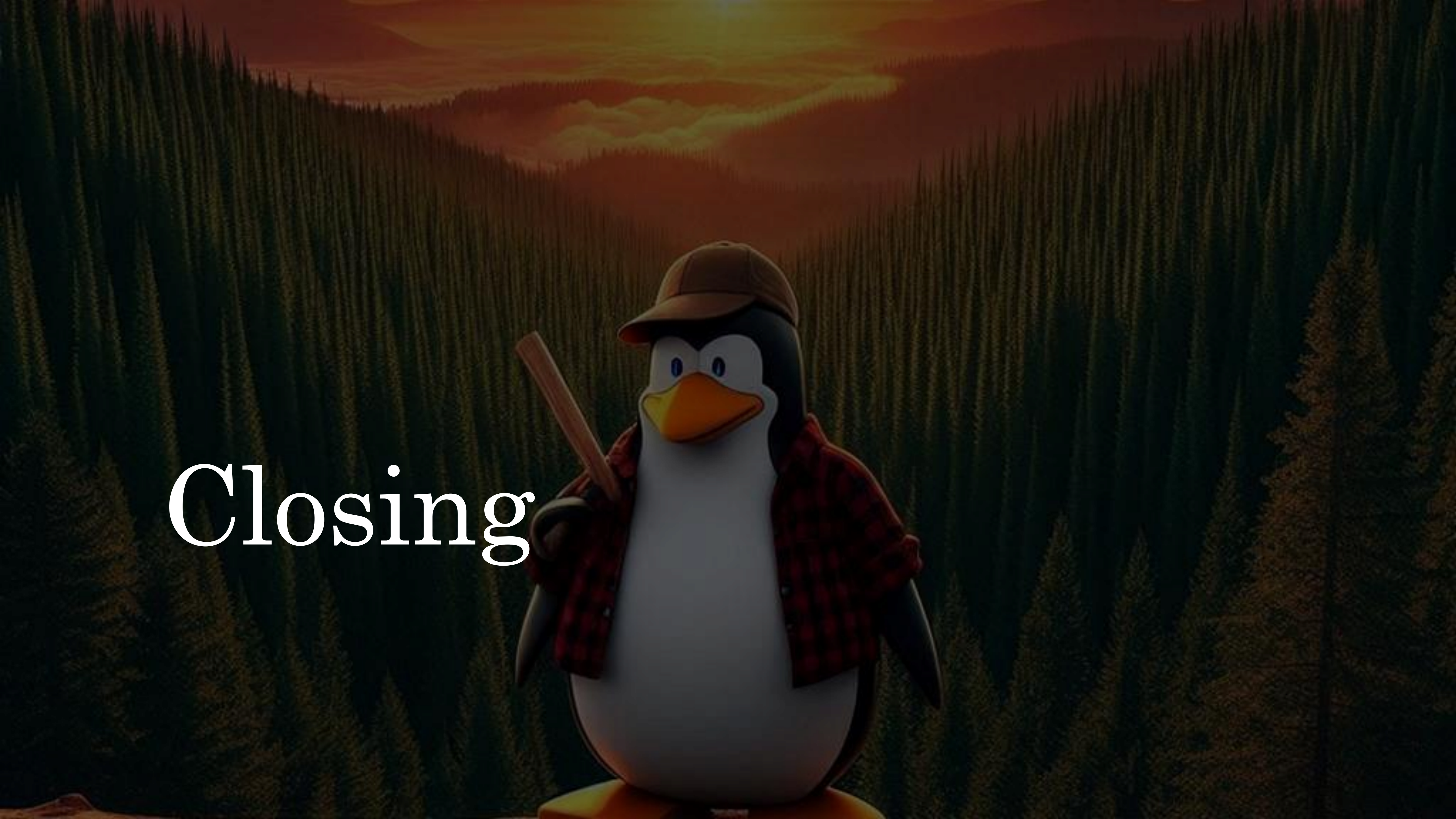
The Lumberjack's Code

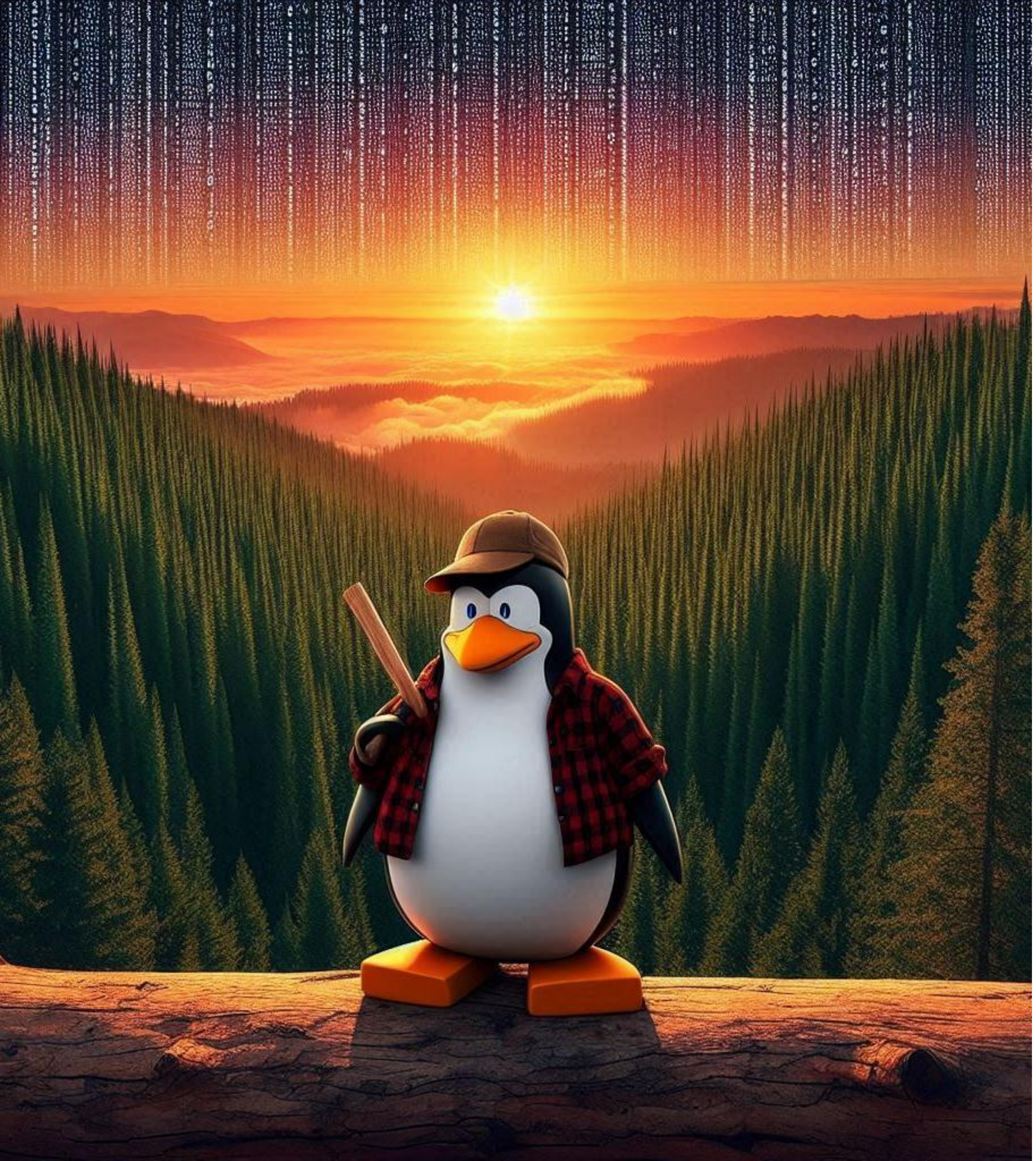
- Structured logging
- Consistent formatting
- Proper error handling

Sustainable Logging

- Resource Management
- - Log Rotation
- - Cleanup Policies

Closing





The Journey Continues

- - Key takeaways
- - Resources for learning
- - Contact information
- Graphics: Sunset over binary forest with Tux

Q&A

- - "Let's chop through your questions!"