Drill: Log-based Anomaly Detection for Large-scale Storage Systems Using Source Code Analysis

Di Zhang¹, Chris Egersdoerfer¹, Tabassum Mahmud², Mai Zheng², and Dong Dai¹

¹University of North Carolina at Charlotte
²Iowa State University
Outline

1. Background
2. Challenge
3. Drill Design
4. Evaluation
5. Conclusion
Importance of Anomaly Detection
Workflow of Log-based Anomaly Detection

- Log Collection
- Log Representation
- Pattern Learning
- Online Detection
Workflow of Log-based Anomaly Detection

1. Log Collection
2. Log Representation
3. Pattern Learning
4. Online Detection
Log Representation: Log Index

PCA
SOSP’09
Invariant Mining
ATC’10
DeepLog
CCS’17

00000100:00080000:0.0:1607448618.3
27577:0:2290:0:(recover.c:58:ptlrpc_initiate_recovery()) lustre-OST0000_UUID:
starting recovery

00000100:00080000:0.0:1607448618.3
27580:0:2290:0:(import.c:681:ptlrpc_connect_import()) ffffa139cab87800
lustre-OST0000_UUID: changing import state from DISCONN to CONNECTING

00000100:00080000:0.0:1607448618.3
27589:0:2290:0:(import.c:524:import_select_connection())
lustre-OST0000-osc-MDT0000:
connect to NID 10.0.0.8@tcp last attempt 4296114409
Log Representation: Log Content

00000100:00080000:0.0:1607448618.3 27577:0:2290:0:(recover.c:58:ptlrpc_initiate_recovery()) lustre-OST0000_UUID: starting recovery

00000100:00080000:0.0:1607448618.3 27580:0:2290:0:(import.c:681:ptlrpc_connect_import()) ffffa139cab87800 lustre-OST0000_UUID: changing import state from DISCONN to CONNECTING

00000100:00080000:0.0:1607448618.3 27589:0:2290:0:(import.c:524:import_select_connection()) lustre-OST0000-osc-MDT0000: connect to NID 10.0.0.8@tcp last attempt 4296114409
Outline

1. Background
2. Challenge
3. Drill Design
4. Evaluation
5. Conclusion
Challenge 1: Index-based Unseen Log Issues

A dataset covers 29 unique runtime logs.
In total 956 distinct log statements in the source code.

Log index oversimplifies the representation of logs, missing important and valuable information.
The context of a log statement in the source code could be a strong feature in understanding the nature of the relevant logs.
Drill Overview

Runtime Log Training and Testing

Anomaly Detection (Training and Testing) 3

Vector Sequences

Runtime Logs

04000000:00000000:0.0:1667454631.76
512:0.3263181:15171:cs_p_create(): lustre-03T0062-oss-
MDT0000: Write last used PID:
{0x100026000:0x3160f:0x0}, index 2: 8
04000000:00000000:0.0:1667117382.78
0002:0.3260568:15171:cs_fd_dev.c:1052:cs_fd_c
reate_dev(): lustre-02T0000: Reserve 6 objects in group 0:0 at
10242...

...
Sentiment Feature Builder: Motivation

1. **CNETERR**("Connection to %s at host %pI4h on port %d was "
   2. refused; check that Lustre is running on that node.\n",
   3. libcfs_nid2str(peer_nid), &peer_ip, peer_port);

1. CDEBUG(D_HA, "recovery of %s on %s failed (%d)\n",
   2. obd2cli_tgt(imp->imp_obd),
   3. (char *)imp->imp_connection->c_remote_uuid.uuid, rc);

1. CDEBUG(D_HA, "%s: reserve %d objects in group %\llx"
   2. at %\llu\n", ofd_name(ofd),
   3. count, seq, next_id);

1. CDEBUG(D_HA, "%s: Wrote last used FID: "DFID", index %d: %\d\n",
   2. d->opd_obd->obd_name, PFID(fid), d->opd_index, rc);

1. CDEBUG(D_NET,"%s Route resolved: %d\n",
   2. libcfs_nid2str(peer_ni->ibp_nid), event->status);

1. CDEBUG(D_HA, "%s: transno %lld is committed\n",
   2. ccb->llcc_tgt->lut_obd->obd_name, ccb->llcc_transno);
Sentiment Feature Builder: Design

- **No Labels**
- **With Labels: Log Level**
- **Labels may be biased**

- **With Labels**
- **Labels are more generic**

Diagram:
- Runtime Logs → Sentiment Model Trainer
- Log Statements from Source Code
- Log Statements from other systems' Source Code
Context Feature Builder: Motivation

```c
rc = some_function();
if (rc) {
    log();
}
```

```c
rc = ostid_set_id(&oa->o_i, ostid_id(&oinfo->loi_oic);
if (rc) {
    ERROR("Bad %lu to set DOSTID : rc %d\n", (unsigned long long)ostid_id(&oinfo->loi_oic),
    POSTID(&oa->o_i), rc);
    ...
}
```

```c
rc = kgnlind_find_and_cancel_dgram(peer->gnp_net->gnn_dev,
    peer->gnp_nid);
if (rc) {
    LCONSOLE_INFO("Received NAK from %s for %s erro %d; "
    "canceled pending connect request\n",
    libcfs_nid2str(conreq->gnr_srcnid),
    libcfs_nid2str(conreq->gnr_dsnid), errno);
    ...
}
```
Context Feature Builder: Design

```c
1  rc = mdt_attr_get_complex(info, mo, ma); /* ReturnTypeI: check rc */
2  if (rc) {
3      CERROR("file attribute read error for "DFID": %d.\n",
4     PFID(mdt_object_fid(mo), rc); /* MessageType: variable checking */
5     RETURN(rc); /* ReturnTypeII: immediately return */
6  }
... /* ControlType: if */
```
Outline

1. Background
2. Challenge
3. Drill Design
4. Evaluation
5. Conclusion
• How is the impact of **sentiment feature**?
• How is the impact of **context feature**?

**Evaluation Outline**

• How is the performance of Drill on **different systems**?
• How is the performance of Drill on **streaming analytics**?

Is Drill robust on **partial training data**?
Evaluation Outline

- How is the impact of **sentiment feature**?
- How is the impact of **context feature**?

- How is the performance of Drill on **different systems**?
- How is the performance of Drill on **streaming analytics**?

Is Drill robust on **partial training data**?
Impact of Sentiment Features

The volume of domain-specific data is not enough to finetune a workable language model.
Drill on Different Systems

Drill achieves the best performance among all the six approaches on F-measure, presenting its effectiveness.
Conclusion and Future Work

- **Conclusion:**
  - We propose to use a storage system-specific sentiment language model and context-based feature extraction to detect the anomaly and show its effectiveness.
  - Our evaluations show Drill outperforms state-of-the-art approaches on two representative large-scale storage systems, HDFS and Lustre.

- **Future Work:**
  - Explore the possibility to consider more features besides the log statement description.
  - Apply more sophisticated language models, such as BERT for sentiment analysis.

Github Repo
- [Code]
- [Dataset]
Q&A

Thank you!
Backup: Use ChatGPT to detect anomaly in log.
Backup: Use ChatGPT to detect anomaly in log.

Log Lines

00000004:00008000:0:0.1607317389.467053:0.5483:0.(osp_object_c:1517:osp_create()) lustre-OST0000-osc-MDT0000:
  Wrote last used FID: [0x1000000000.0x4c2b:0x0], index 0: 0 |]
00000004:00008000:0:0.1607317389.467055:0.5483:0.(osp_object_c:1517:osp_create()) lustre-OST0000-osc-MDT0000:
  Wrote last used FID: [0x1000000000.0x4c2b:0x0], index 1: 0 |]
00000004:00008000:0:0.1607317389.467056:0.5483:0.(osp_object_c:1517:osp_create()) lustre-OST0000-osc-MDT0000:
  Wrote last used FID: [0x1000000000.0x4c2b:0x0], index 2: 0 |]
00000004:00008000:0:0.1607317389.469131:0.5423:0.(osd_handler_c:1588:osd_trans_commit_cb()) transaction
    @0x8f9676cbe899a0 commit error: 2 |]
00000004:00008000:0:0.1607317389.469136:0.5423:0.(osd_handler_c:1588:osd_trans_commit_cb()) transaction
    @0x8f9676cbe899c0 commit error: 2 |]
00000004:00008000:0:0.1607317389.469137:0.5423:0.(osd_handler_c:1588:osd_trans_commit_cb()) transaction
    @0x8f9676cbe899c0 commit error: 2 |]
00000004:00008000:0:0.1607317389.469138:0.5423:0.(osd_handler_c:1588:osd_trans_commit_cb()) transaction
    @0x8f9676cbe899c0 commit error: 2 |]
00000004:00008000:0:0.1607317389.469139:0.5423:0.(osd_handler_c:1588:osd_trans_commit_cb()) transaction
    @0x8f9676cbe899c0 commit error: 2 |]
00000004:00008000:0:0.1607317389.469139:0.5423:0.(osd_handler_c:1588:osd_trans_commit_cb()) transaction
    @0x8f9676cbe899c0 commit error: 2 |]

LLM Anomaly Description

Historic Summary: Continuing from the previous logs, Lustre-OST0000, Lustre-OST0001, and Lustre-OST0002 continue to write their last used FIDs to MDT0000 with incremented indexes. Additionally, multiple transactions with commit errors are recorded in the logs. No other significant events are noted.

System Health Prediction: Critical

Description of System Health: The multiple transactions with commit errors indicate a problem with the Lustre file system's ability to commit changes. This could lead to data loss or corruption if not addressed immediately.

Anomalies: [0001111111]

Description: The commit errors in the transactions indicate that Lustre is having issues writing changes to disk. This could cause data inconsistencies or loss and is a critical issue that needs to be addressed.
Backup: Use ChatGPT to detect anomaly in log.
Existing Work: Two Different Ways

**DeepLog**

- Log Index
  - # of 1 = 2
  - # of 2 = 1
  - # of 3 = 2
  - Invariant: # of 1 == # of 3

**Log Content**

- Search keyword, e.g., “error”, “exception”.
- Compare synonyms and antonyms, e.g., LogAnomaly
- BERT-based language model, e.g., NeuralLog

---

**IM**

- # of 1 = 2
- # of 2 = 1
- # of 3 = 2
- Invariant: # of 1 == # of 3
Sentiment Feature Builder: Design

- **No Labels**
  - Log Statements from Source Code
  - Runtime Logs
  - Sentiment Model Trainer
  - Log Statements from other systems’ Source Code

- **With Labels**
  - Log Level
  - Labels may be biased
  - Labels are more generic