PISCES Resiliency Architecture

STUDENTS: Paresh Bapat, Keerthi Pitchapati, Daqian Yao, Bonie Wang, Ruiqi Li, William Chen, Cameron Jennings

PISCES International
Public Infrastructure Security Cyber Education System

B|E|C|U

PISCES

- PISCES - a nonprofit that teaches students from various universities entry-level cyber analyst skills
- The project's beneficiaries include numerous municipalities that depend on PISCES for cybersecurity due to their limited cyber monitoring, investigation, and response resources
- In the event of a failure, the absence of a failover in the system leaves these entities vulnerable

Elastic

- PISCES uses ELK (Elastic Search, Logstash, and Kibana) for real-time data logging, queries, and visualization
- Beats ships lightweight metadata to the stack
- Implementing Elastic's Cross-Cluster Replication (CCR) as the failover mechanism ensures continuous operation

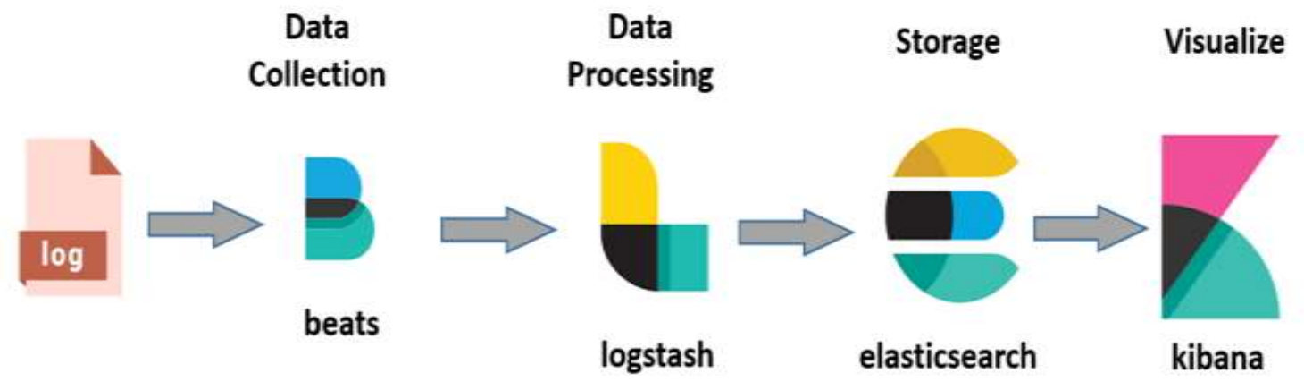


Fig 1: An Overview of Data Flow from Collection to Visualization

Stack Features

- PISCES integrates ELK into their network stack for dynamic logging, monitoring, and analytics
- Students access stack's private network through OpenVPN
- Proxmox is the network manager interface to communicate with the clusters and nodes
- Suricata and the firewall used for intrusion detection system
- Incorporates access controls, authentication mechanisms, and data encryption as security measures
- Leverages Elastic's Cross-Cluster Replication (CCR) and round-robin DNS for efficient failover

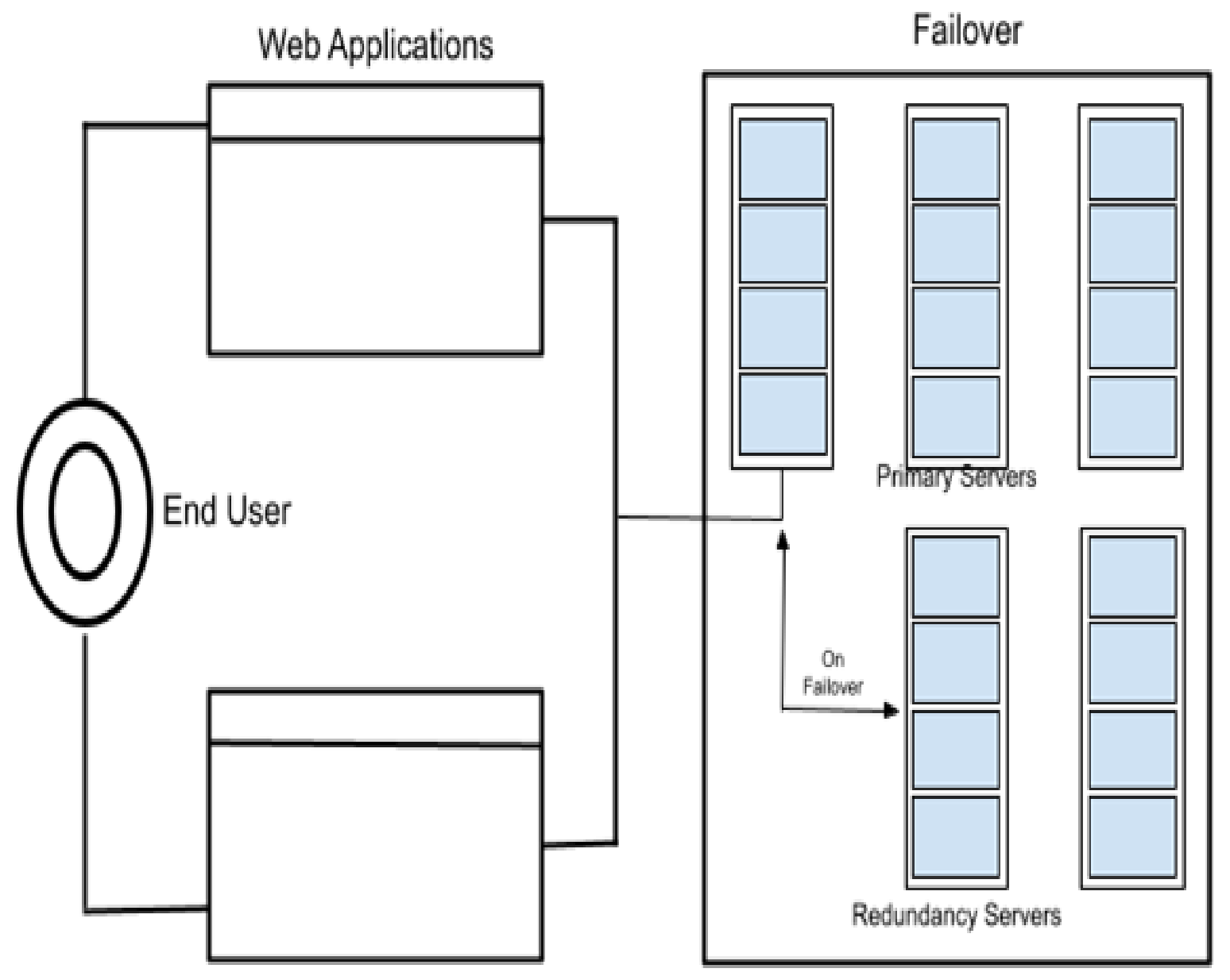


Fig 2: Aggregating Logs from Multiple Applications for ElasticSearch

Backup Server

- The backup servers provides resilience to the PISCES platform
- In the event of a failure of the primary server located in Poulsbo, WA, the backup servers located at the University of Montana assumes it's workload
- It is designed to maintain synchronization with the primary server

Local Cluster

- Local cluster is the Elastic term to refer to backup servers, remote cluster refers to PISCES primary infrastructure
- Unidirectional Cross-Cluster Replication is utilized to replicate data from the remote cluster to the local cluster in near real-time, failover in the event of a failure, and failback once the primary is operational
- As the backup infrastructure at the University of Montana has yet to be built, we simulated our implementation using virtual machines within the Cyber Range Poulsbo

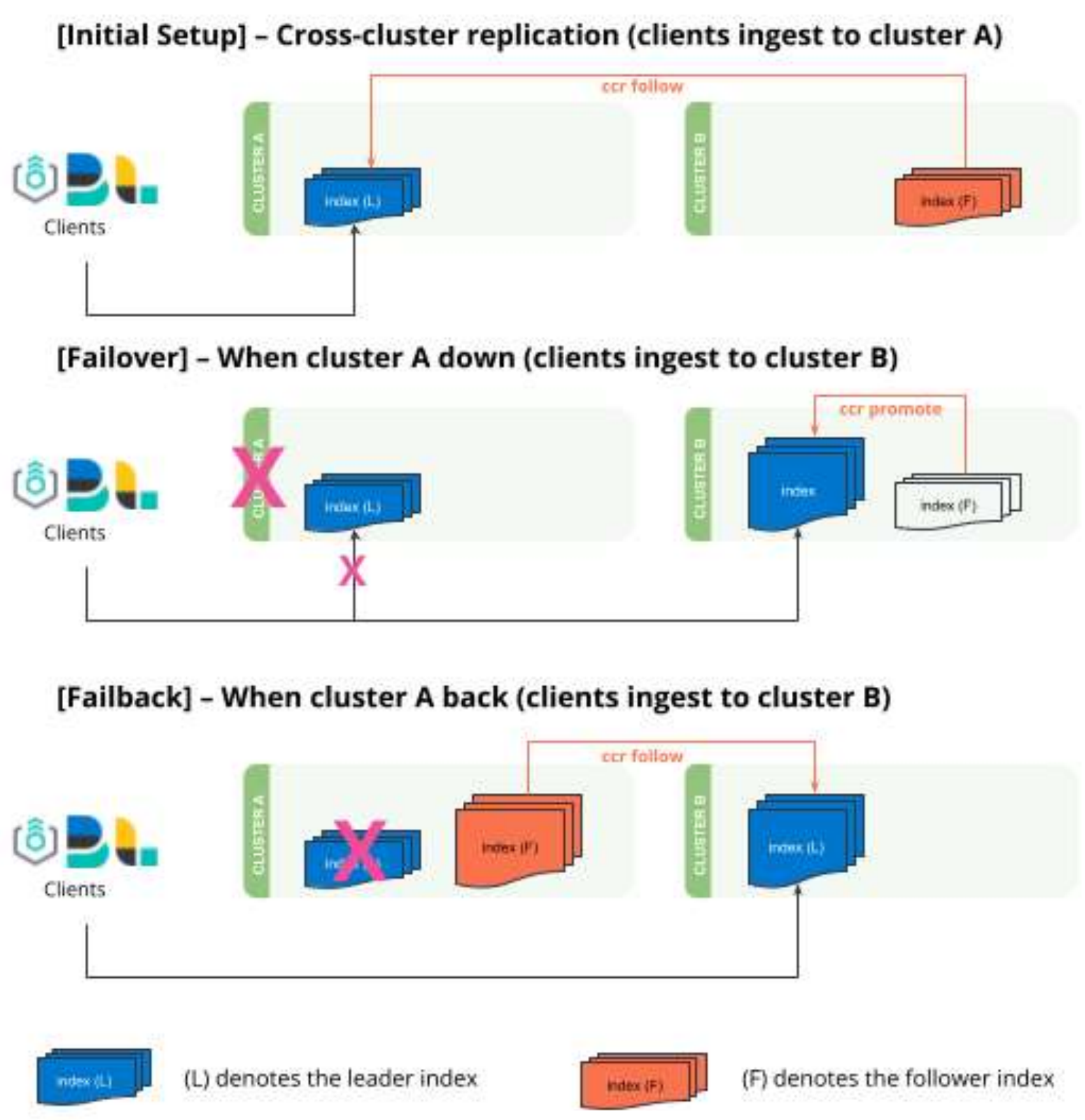

[Initial Setup] – Cross-cluster replication (clients ingest to cluster A)
ccr follow
Clients
CLUSTER A
CLUSTER B
index (L)
index (F)
[Failover] – When cluster A down (clients ingest to cluster B)
ccr promote
index
X
[Failback] – When cluster A back (clients ingest to cluster B)
(L) denotes the leader index
(F) denotes the follower index

Fig 3: Setup, Failover, and Failback Process

[1]

Data Streams

- Stack ingests metadata forwarded from collectors within the municipalities network
- Students can then access data and try to detect malicious activity
- Data streams must be redirected to backup servers domain in the event of an outage
- Round-robin DNS used to substitute the backup servers' domain name when a failure is detected by the system, ensuring continuous logging of data

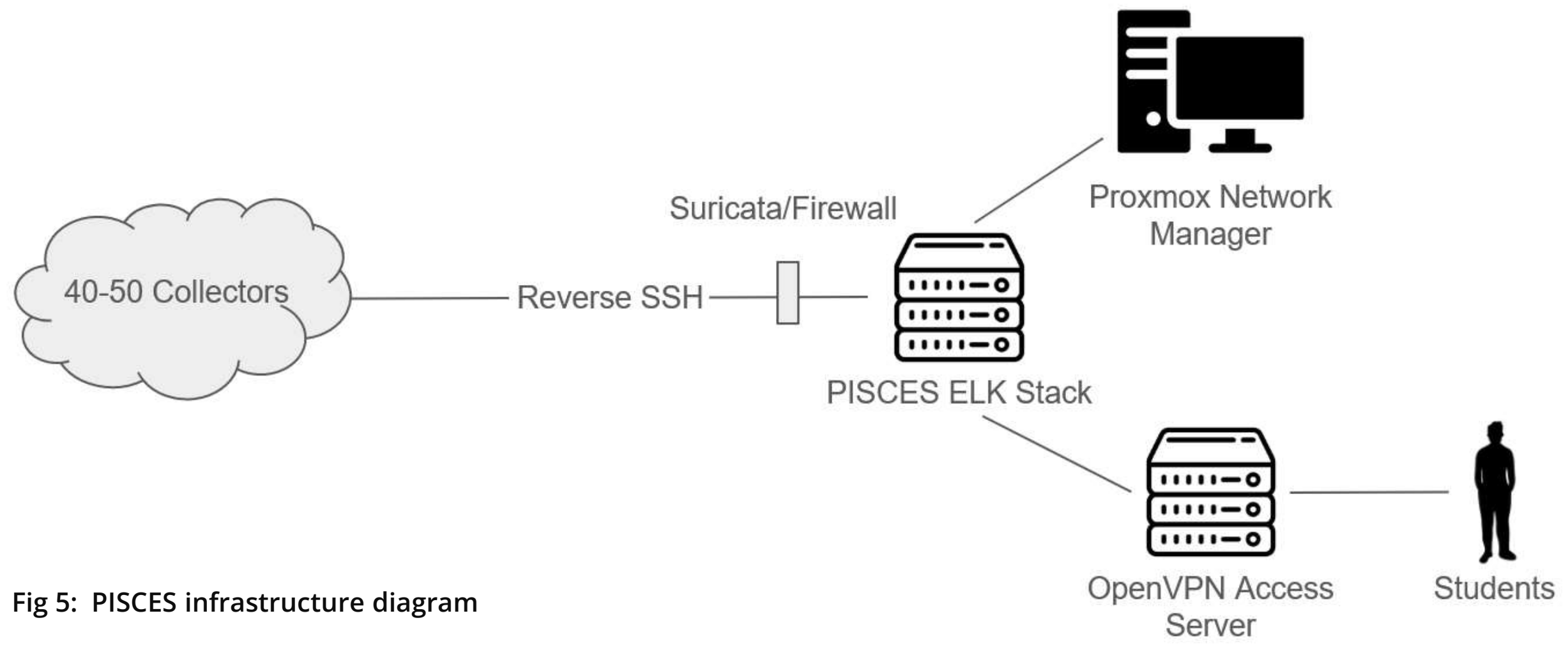
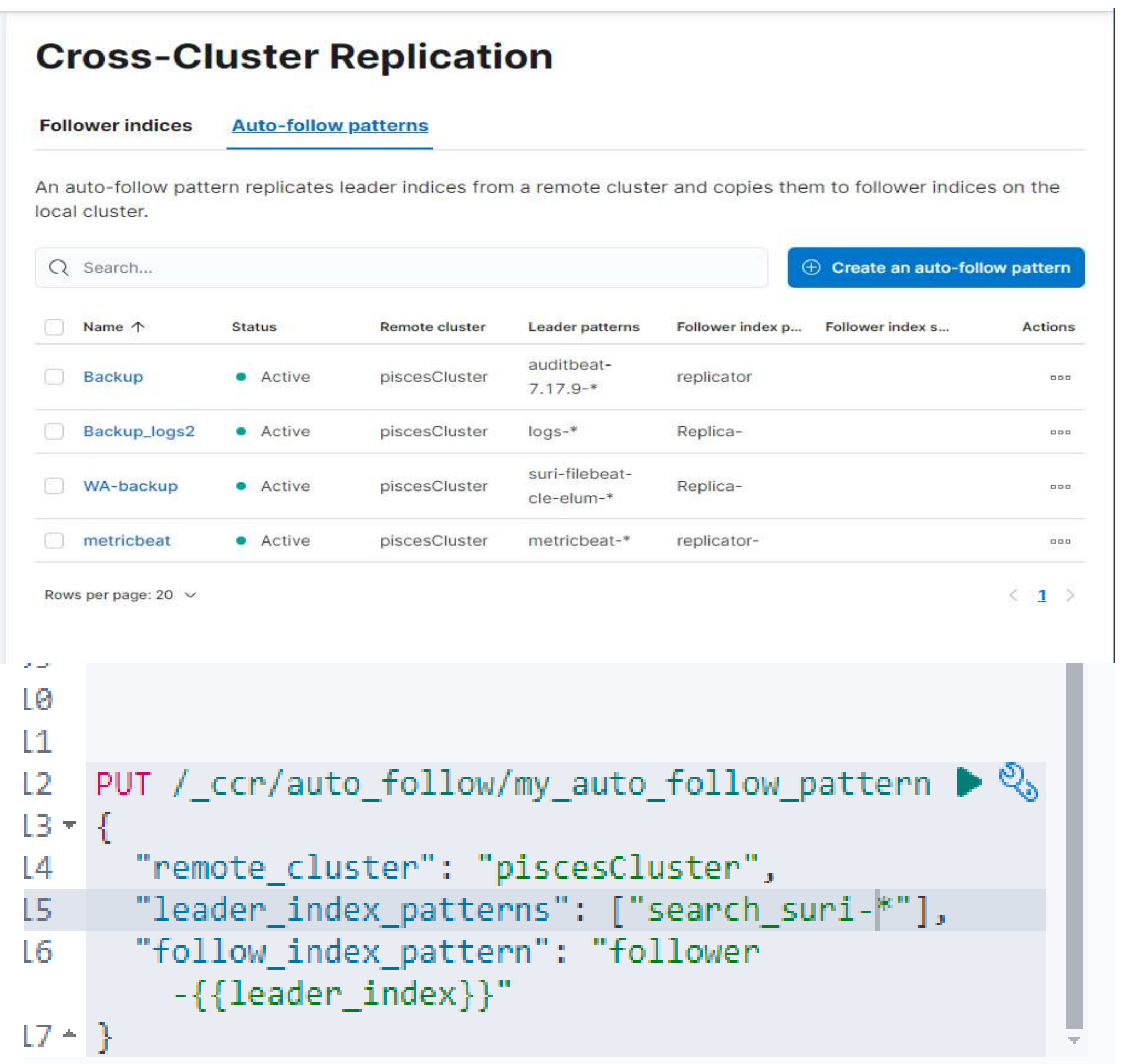


Fig 5: PISCES infrastructure diagram

Cross-Cluster Replication

- Proxmox enables us to configure the remote and local clusters within the console to initialize CCR within the YAML files serving as configuration files for Elastic
- Primary and backup servers running Elastic are able to recognize each other and assume specific roles to ensure replication and continuous operation
- Current PISCES cluster is dedicated to leader indices and new backup cluster for follower indices
- An auto-follow pattern replicates data from leader to follower
- If an outage occurs, backup cluster assumes the roles and the collectors begin to forward data to it
- Once operational, the PISCES cluster should first replicate data then assume its roles back



Cross-Cluster Replication

An auto-follow pattern replicates leader indices from a remote cluster and copies them to follower indices on the local cluster.

Name ↑	Status	Remote cluster	Leader patterns	Follower index p...	Follower index s...	Actions
Backup	● Active	piscesCluster	auditbeat-7.17.9-*	replicator		▫▫▫
Backup_logs2	● Active	piscesCluster	logs-*	Replica-		▫▫▫
WA-backup	● Active	piscesCluster	suri-filebeat-cle-elum-*	Replica-		▫▫▫
metricbeat	● Active	piscesCluster	metricbeat-*	replicator-		▫▫▫

Rows per page: 20

```
PUT /_ccr/auto_follow/my_auto_follow_pattern
{
  "remote_cluster": "piscesCluster",
  "leader_index_patterns": ["search_suri-*"],
  "follow_index_pattern": "follower
    -{{leader_index}}"
}
```

Fig 5: Setting Up Auto-Follow Patterns for Cross-Cluster Replication in Elasticsearch

- Four nodes actively replicating the leader indices
- Primary recognizes that CCR has been initialized and the followers are referenced

Future Work, References, and Acknowledgments

- Upgrade Elastic package for more features
- Write scripts to handle the transfer of data streams
- Configure OpenVPN to allow students to access backup

[1]"Tutorial: Disaster recovery based on uni-directional cross-cluster replication: Elasticsearch Guide [8.13]," Elastic, https://www.elastic.co/guide/en/elasticsearch/reference/current/ccr-disaster-recovery-uni-directional-tutorial.html

ELECTRICAL & COMPUTER ENGINEERING
UNIVERSITY of WASHINGTON

Industry Mentors: Mike Hamilton, Deborah Wells, Dillion Kierce

Faculty Mentors: Radha Poovendran & Kavya Balsubmaranian

Sponsors: PISCES & BECU