LogPoint Architecture (Reference)

Date: 2026-02-26
Source: Business expertise

Node Types

1. Data Node (DN)

Composition: Collector + Storage
Role: Log ingestion and storage
API Configurable: ✅ Yes

2. Search Head (SH)

Composition: Web interface + search engine + alerting
Role: Queries, dashboards, alerts
API Configurable: ✅ Yes

3. AIO (All-In-One)

Composition: Data Node + Search Head on single machine
Role: Monolithic SIEM
API Configurable: ✅ Yes (as DN + SH combined)

Deployment Types

Client A: AIO Only

```
Client A
└── AIO-01 (all configuration)
```

Client B: Simple Distributed

```
Client B
├── DN-01 (storage + collection site A)
├── DN-02 (storage + collection site B)
└── SH-01 (single interface for both DNs)
```

Client C: Distributed with Clustering

```
Client C
├── DataNode Cluster "production"
│   ├── DN-PROD-01
│   ├── DN-PROD-02
│   └── DN-PROD-03 (same config as others)
│
├── DataNode Cluster "archive"
│   └── DN-ARCHIVE-01 (different config from prod)
│
├── SearchHead Cluster "frontend"
│   ├── SH-01
│   └── SH-02 (same config, load balancing)
│
└── SH-Admin (dedicated admin search head, not in cluster)
```

Config ↔ Node Type Mapping

Config Type	Data Node	Search Head	AIO	Comment
Repos	✅	×	✅ (DN part)	Physical storage
Routing Policies	✅	×	✅ (DN part)	Log routing
Normalization Policies	✅	×	✅ (DN part)	Log parsing
Processing Policies	✅	×	✅ (DN part)	Processing pipeline
Device/Log Sources	✅	×	✅ (DN part)	Log sources
Alert Rules	×	✅	✅ (SH part)	Threat detection
Dashboards	×	✅	✅ (SH part)	Visualization
Reports	×	✅	✅ (SH part)	Periodic reports
Users/Permissions	✅	✅	✅	Authentication everywhere
System Settings	✅	✅	✅	SNMP, backup, etc.

Key CaC-ConfigMgr CaC Concepts

Pseudo-Cluster

Group of **same-type nodes** receiving the **same configuration**.

- **DataNodeCluster**: 1..N Data Nodes identical (HA, load balancing)
- **SearchHeadCluster**: 1..N Search Heads identical (HA, query concurrency)

Cross-References

- A Search Head can be connected to **1 or more** DataNodeClusters
- A client can have **multiple** DataNodeClusters (prod, archive, test...)

Configuration Granularity

- Config can target: **individual AIO**, **individual DN**, **individual SH**
- Config can target: **entire cluster** (applied to all members)
- Config can target: **entire client** (users, global settings)

Immutable Rule

Config elements are **associated by node type**:

- Repos can only be deployed on Data Nodes
- Alerts can only be deployed on Search Heads
- Users go everywhere

Note: An AIO = DataNode + SearchHead combined