### Cluster

#### Overview

Logpresso Sonar supports cluster configurations. A cluster consists of independent nodes that collaborate to perform roles such as data collection, analysis, and forwarding, while providing redundancy configurations for each node to enhance system stability and availability.

In Logpresso Cloud, instances of Logpresso Sonar are automatically configured as clusters. In on-premises environments, they can be configured as standalone or cluster forms according to operational needs, so changes to cluster settings are not recommended.

Architecture

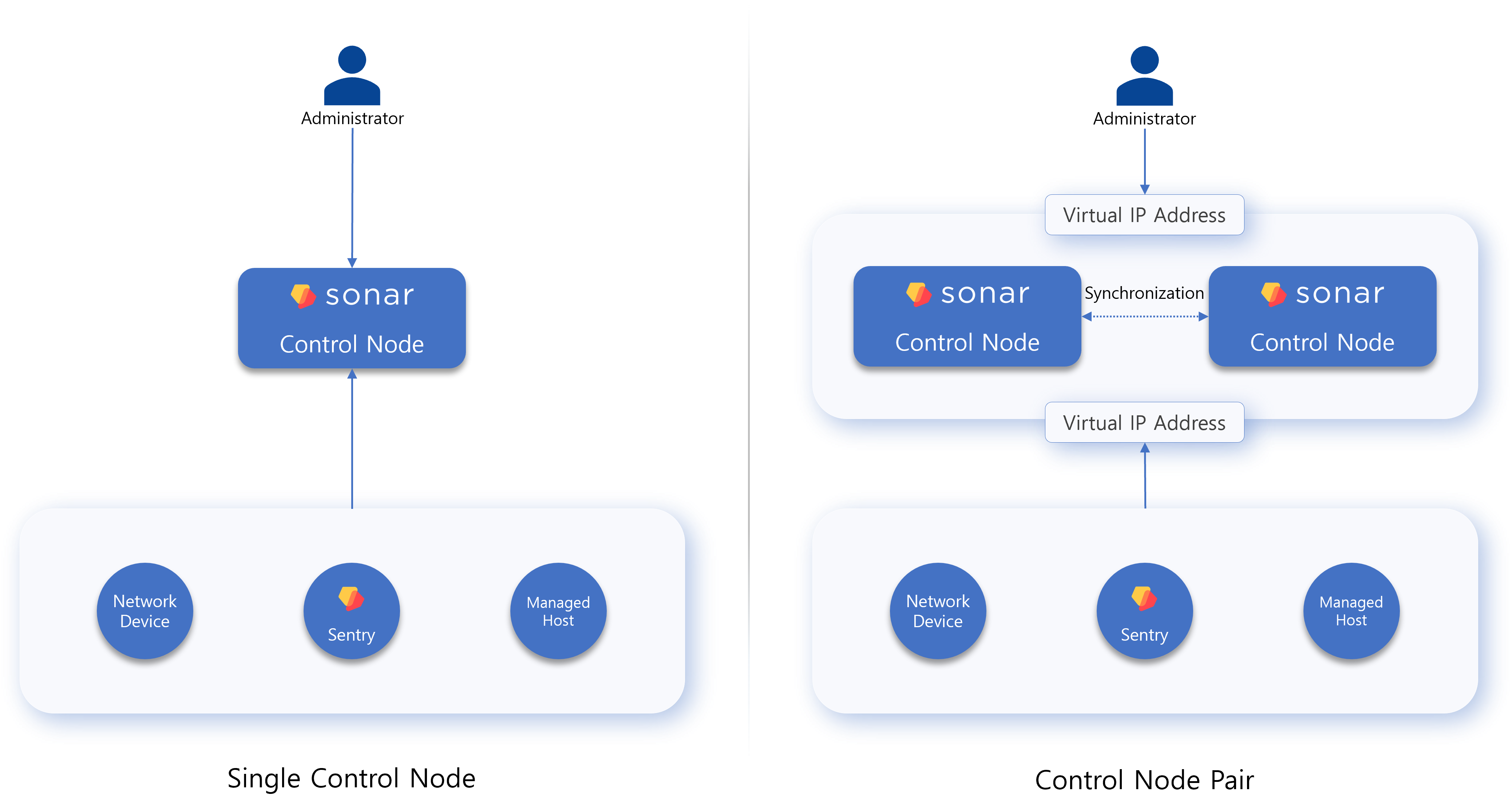
Logpresso clusters can be categorized based on the tiers they comprise:

* **1 Tier**: A tier composed solely of control nodes.
* **2 Tier**: Forwarder node - control node.
* **2 Tier (Legacy)**: Data node - control node.
* **3 Tier**: Forwarder node - data node - control node.

You can select an appropriate tier configuration based on the volume of original logs collected daily. Logpresso **recommends a 3-tier architecture**.

1 Tier: Control Node Tier

The 1-tier configuration is illustrated as follows. The left side shows a single control node, while the right side depicts a pair of control nodes. Based on Logpresso's reference hardware, it can process up to 200GB of data per day.



**Single Control Node**

If the amount of data to be collected is small, a **single server** can perform both the data node and control node functions simultaneously. However, data loss may occur in the event of a node failure.

**Control Node Pair**

This is a Tier-1 high-availability (HA) configuration in which two control nodes are deployed redundantly to ensure service continuity in the event of a failure.

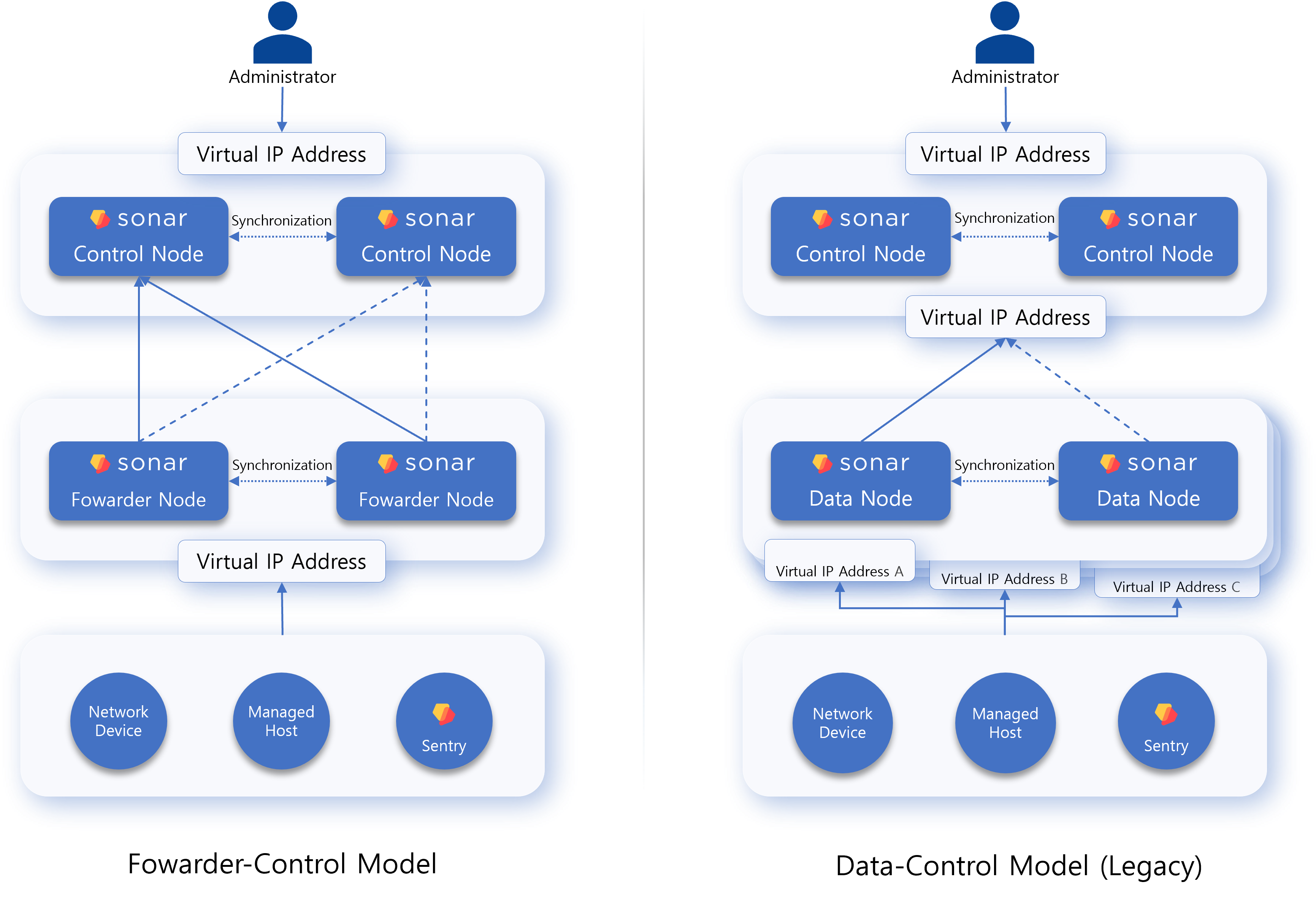
**Each node shares a virtual IP address**, so external systems can access the cluster using either the virtual IP or a domain name associated with the control node.

* When network devices, managed hosts, or sentries transmit data, the active node receives the data.
* When an administrator accesses the system, the active node provides access to the web console.

Since control node pairs cannot be horizontally scaled, it is advisable to switch to a 3-tier configuration if the amount of data to be collected increases.

2 Tier: Forwarder-Control Node / Data Node-Control Node (Legacy)

The 2-tier configuration separates the nodes that collect data from those that store it. The left side of the following diagram shows the forwarder-control model, while the right side depicts the data-control model (legacy).



**Forwarder-Control Model**

This is an extension of the 1-tier architecture composed of control nodes with an added pair of forwarder nodes, which is the basic configuration seen in [Logpresso Cloud](https://logpresso.cloud/). Forwarder nodes were introduced in version 4.0.2404.0 and function as data gateways and load balancers ([related document](https://docs.logpresso.comnull)). Both forwarder and control nodes are recommended to be configured with redundancy for availability.

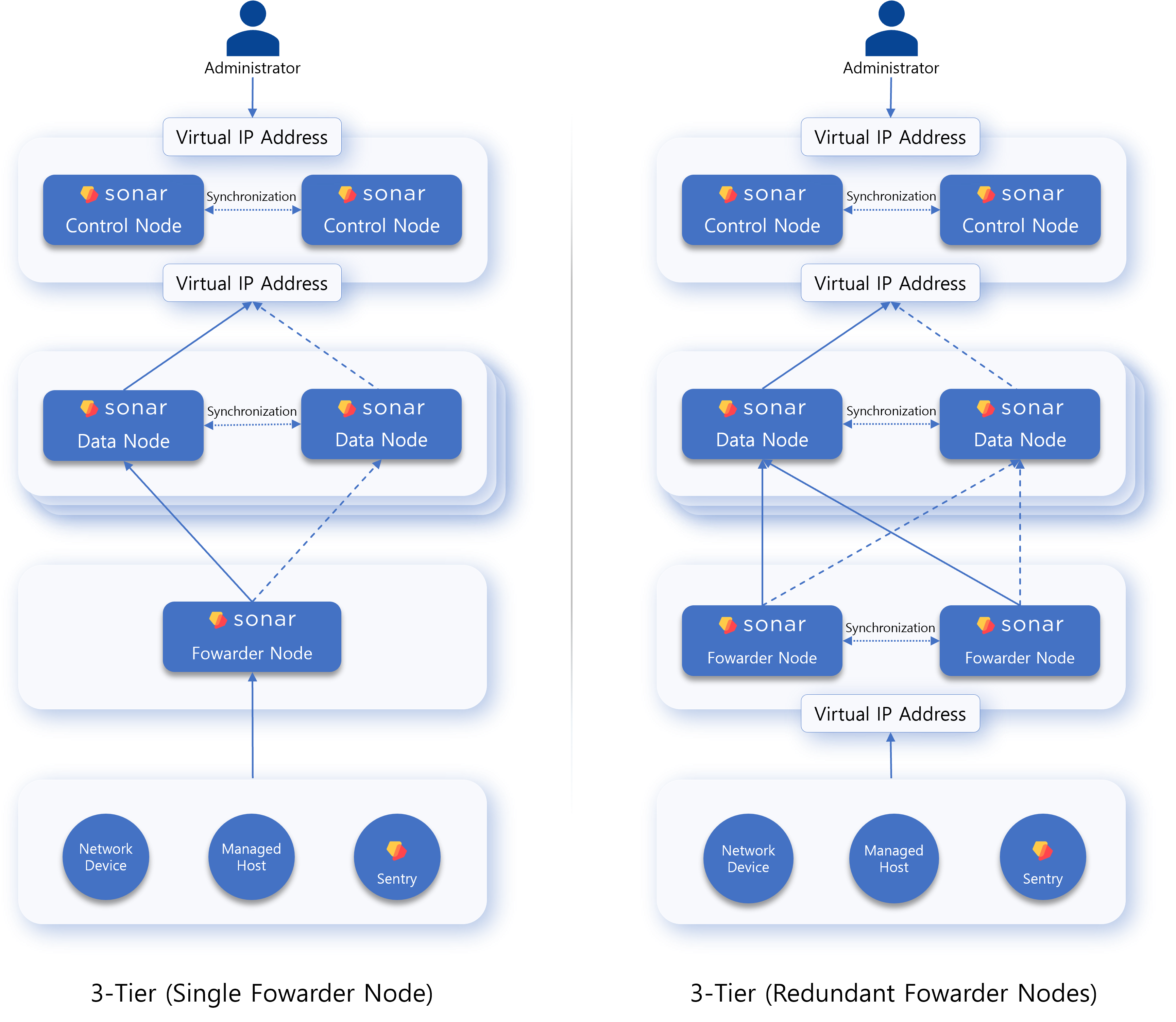
Forwarder nodes are used considering the horizontal scaling of downstream nodes, making this configuration a transitional form of the 3-tier architecture. Since only one pair of control nodes can be used, horizontal scaling requires changing the entire configuration to a 3-tier setup.

**Data-Control Model (Legacy)**

This architecture was used prior to version 4.0.2404.0, adding a pair of data nodes to the 1-tier configuration. By distinguishing between the tiers that perform data collection and analysis, it allows for horizontal scaling at the data node pair level, providing flexibility even as the amount of data collected increases. However, since each data source (network devices, managed hosts, sentries) must communicate with a designated pair of data nodes, the network topology becomes increasingly complex as the number of data node pairs increases, making this configuration less recommended.

3 Tier: Forwarder-Data-Control (Recommended Configuration)

The 3-tier forwarder-data-control model is a new architecture that replaces the 2-tier data-control model (legacy) and is the recommended cluster configuration for large-scale data collection environments.



The 3-tier configuration overcomes all the disadvantages of the 2-tier configuration. If there are two or more data node pairs, a forwarder node must be configured. The forwarder node can resolve the topology issues present in the 2-tier data-control model.

Transitioning from Legacy to 3 Tier Architecture

To transition from a legacy architecture to a 3-tier architecture:

Install Forwarder Node: Bring the forwarder node into the operational environment and install it.

Reinstall Apps: Since apps are not installed on the forwarder node, you must install them on the forwarder server if necessary through [app reinstallation](https://docs.logpresso.comnull).

Replace Loggers: Different approaches are needed based on the [collection methods of the loggers](https://docs.logpresso.comnull).**Passive Logger**: Configure a new logger and stop/delete the legacy logger.

Configure the logger with the collection location as the forwarder node pair and the loading location as the data node pair.

Change the data transmission destination from the data source to the virtual IP address or domain address of the forwarder node and check the collection status.

If there are no issues, stop or remove the legacy logger.**Active Logger**: Stop the legacy logger and configure a new logger.

Stop the legacy logger running on the data node.

Configure the logger with the collection location as the forwarder node pair and the loading location as the data node pair, then check the collection status.

If there are no issues, remove the legacy logger as needed.

Node Types

The Logpresso cluster consists of control nodes, data nodes, and forwarder nodes. A standalone Logpresso Sonar server performs the roles of both data and control nodes.

Control Node

The control node manages all nodes in the Logpresso cluster and provides a web console for user access to the cluster. Redundant control nodes share a virtual IP address.

**Node Control**

Forwarder and data nodes request settings and policy synchronization using the control node's virtual IP address, and the control node communicates with each node through a polling mechanism to send modified settings or policies based on their requests.

**User Web Interface**

Users can also access the web console using the virtual IP or domain address of the control node. The web access address for employees who receive explanation requests due to policy violations or approvers who need to review explanations also utilizes this virtual IP address.

**Data Analysis and Detection of Security Threats and Anomalies**

The control node performs actions based on the data loaded in the data nodes according to [stream rule](https://docs.logpresso.comnull) and [batch rule](https://docs.logpresso.comnull) scenarios, including:

* Detection of security threats or anomaly [events](https://docs.logpresso.comnull)
* Issuance and management of [tickets](https://docs.logpresso.comnull)
* [Explanation Requests](https://docs.logpresso.comnull) and approval management
* [Automated responses](https://docs.logpresso.comnull) to detected threats

Most Logpresso queries executed by users on the control node or periodically run in the Logpresso cluster read and process data from the data nodes. The control node establishes and manages the execution plans for Logpresso queries and processes the data after receiving the distributed results from each node.

The control node uses MariaDB for on-premises environments and managed databases in the cloud.

Data Node

The data node parses, normalizes, indexes, and stores the data collected through loggers in [tables](https://docs.logpresso.comnull).

**Data Loading and Query Execution**

Parsing of original data by [parsers](https://docs.logpresso.comnull) and normalization defined in [logger models](https://docs.logpresso.comnull) all occur at the data node.

All data nodes store original and normalized data together in tables with the same name. When Logpresso queries are executed on the control node, data retrieval commands such as [table](https://docs.logpresso.comnull) and [fulltext](https://docs.logpresso.comnull) are processed in parallel across each data node.

Lifecycle Management: The data node manages data according to the defined [retention period](https://docs.logpresso.comnull) and [data lifecycle](https://docs.logpresso.comnull) in the tables.

Forwarder Node

The forwarder node was introduced in version 4.0.2404.0 ([related document](https://docs.logpresso.comnull)). Redundant forwarder nodes also share a virtual IP address like control nodes.

- It is recommended to configure a forwarder node when there are two or more data node pairs.- To operate data node pairs in an active-active manner, an L4 switch or network load balancer is required.

**Data Gateway**

[Loggers](https://docs.logpresso.comnull) run on the forwarder node, which acts as the data transmission gateway for the Logpresso cluster. The virtual IP address or domain address of the forwarder node is used as the gateway address.

While a data node can perform the role of a data gateway instead of a forwarder node, this is not recommended. The number of data gateways increases with the number of data node pairs, and the data source must designate only one of them for data transmission, complicating the network structure.

**Load Balancing**

The data received/collected by the forwarder node is transmitted to the data nodes. The forwarder node performs load balancing to ensure that data is evenly distributed across multiple data node pairs according to the transmission methods defined in the [loggers](https://docs.logpresso.comnull), or it can send data to specific node pairs.

If the forwarder node detects a failure while communicating with the data nodes, it temporarily stores the data to be transmitted in memory and on the local disk, and upon recovery of the failure, it retransmits the stored data to the data nodes. After completing the transmission, the forwarder node removes any remaining data from local storage.

Configuration Order

When configuring a cluster, set up the nodes in the following order:

Control Node and Redundancy

Data Node and Redundancy

Forwarder Node and Redundancy

This document only covers the usage of the web console, while the actual installation process will be provided in a separate document.

* The installation process for control and data nodes will be provided in a separate document.
* For the installation and configuration process of the forwarder node, please refer to [this document](https://docs.logpresso.comnull).

Data Lifecycle

The data lifecycle generally refers to the series of processes from data creation to deletion. Logpresso Sonar collects data from sources such as logs and PCAP files, which are generated in chronological order. This data is characterized by its increasing importance the closer it is to the 'present'.

As the volume of stored data increases, so do the storage costs. The storage lifecycle feature allows frequently accessed recent data to be stored on fast but expensive storage, while infrequently accessed older data can be stored on slower but cheaper storage, providing a way to balance performance and cost.

Even when the location of stored data changes or is in the process of being changed, the data retrieval/analysis functionality operates the same way as when using a single storage, thus having no impact on system operation and usage.

The data lifecycle applies only to collected data and does not apply to the system data of the nodes that make up the cluster.

Storage Tiers

Logpresso Sonar supports storage tiering, where frequently accessed recent data is stored on the highest performance storage (SSD), and infrequently accessed older data is stored on relatively lower performance but cheaper storage (NAS, cloud object storage).

The storage in Logpresso Sonar is composed of three tiers.

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Hot (Tier 1) | Warm (Tier 2) | Cold (Tier 3) |
| Device Type | NVMe, SSD | HDD, WORM | WORM, NAS, cloud object storage |
| Search Performance | Very High | Average | Low |
| Statistical Performance | High | Average | Low |
| Replication Factor | 2 | 2 | 1 |
| Unit Cost | High | Average | Low |
| Configuration Purpose | Maximize search performance | General analysis | Data archiving, compliance adherence |

**Hot**

The highest tier that stores collected data first, utilizing high-cost, high-performance storage. After the configured period, data rolls over to the lower tier (Warm or Cold).

**Warm**

Intermediate cost and performance storage that holds data rolled over from the **Hot** tier. If nodes are redundant, **Node A and Node B each perform the rollover**, resulting in each piece of data being replicated once.

**Cold**

Low-cost, low-performance storage that holds data rolled over from the **Hot** and **Warm** tiers. Even if nodes are redundant, **only one copy of the data is rolled over**.

The **Cold** tier is typically used to store older data required for compliance or to retain data with low utility and very infrequent access.

Depending on the operational environment and purpose, **Warm** and **Cold** tiers can be applied selectively. To use WORM storage, you need to obtain a WORM driver from Logpresso Store.

When using NFS in the Warm and Cold directories, ensure that the data transfer speed is adequately guaranteed.

Rollover

Rollover is the action of moving data to a lower tier based on its retention period or capacity. For example, if a retention period of 120 days is specified for each of the **Hot**, **Warm**, and **Cold** tiers, data will undergo a total of 360 days of retention across each tier. Once the retention period in the **Cold** tier is reached, data will be deleted or permanently archived according to the settings defined for that tier.



* Rollover applies to collected data, while system data is always retained in the **Hot** tier.
* You can limit the speed of data transfer between storage tiers and execution schedules in the [rollover settings](https://docs.logpresso.comnull).
* You can specify the [maximum storage capacity](https://docs.logpresso.comnull). Each node checks the maximum storage capacity every 15 minutes, and if the stored data exceeds the maximum capacity, the excess data will roll over to the lower storage tier.

Logpresso Sonar operates as follows to prevent data loss during rollover:

It duplicates the files to be sent to the lower tier as temporary files.

Once file duplication is complete, it deletes the files from the upper storage and renames the temporary files to match the originals.

If the lower tier storage is WORM or cloud storage, you can configure it to transfer files without temporary file duplication.

Differences from Existing Features

The data lifecycle is similar to the [retention period](https://docs.logpresso.comnull) of tables and the [storage management](https://docs.logpresso.comnull) of nodes, but there are key differences:

|  |  |  |
| --- | --- | --- |
| Category | Table Retention Period | Lifecycle |
| Scope of Application | Data within individual tables (local setting) | All data recorded in storage (global setting) |
| Management Target | Data at the table partition level | Data at the table partition level |
| Retention Expiry | Data deletion | Rollover to lower storage tier |
| Storage Management | Deletion of old data or cessation of collection | (1st) Rollover, (2nd) deletion or archiving |

The data lifecycle and table retention period operate independently. The shorter of the two specified data retention periods will apply, so choose one of the following methods for data management:

Use only the data lifecycle

* Keep the default setting of "permanent storage" for the retention period when creating tables.
* Data management based on the lifecycle is easier than table-level management since it is a global setting.

Use the data lifecycle as the primary function and the table retention period as a secondary function

* Specify the retention period for the data lifecycle as a global setting.
* Set the table retention period shorter than the global setting only when necessary.

Initial Values for Lifecycle

No initial values are set by default. In this state, data will operate according to the retention period of the tables and the storage management settings of the nodes.

[Retention period](https://docs.logpresso.comnull) defined in **Table** settings: Deletes or permanently archives data that exceeds the retention period.

[Storage management](https://docs.logpresso.comnull) defined in **Node** settings: Deletes old data or ceases data collection before local storage reaches saturation. The monitored storage in this case is the partition where Logpresso's data storage directory resides.