### クラスター

#### 概要

ログプレッソ・ソナーはクラスター構成をサポートしています。クラスターは独立したノードで構成され、データ収集、分析、転送などの役割を協調して実行し、各ノードごとに冗長構成を提供することで、システムの安定性と可用性を高めます。

ログプレッソ・クラウドでは、ログプレッソ・ソナーのインスタンスが自動的にクラスターとして構成されます。オンプレミス環境では、運用要件に応じてスタンドアロンまたはクラスター構成を選択できますが、クラスター設定の変更は推奨されません。

アーキテクチャ

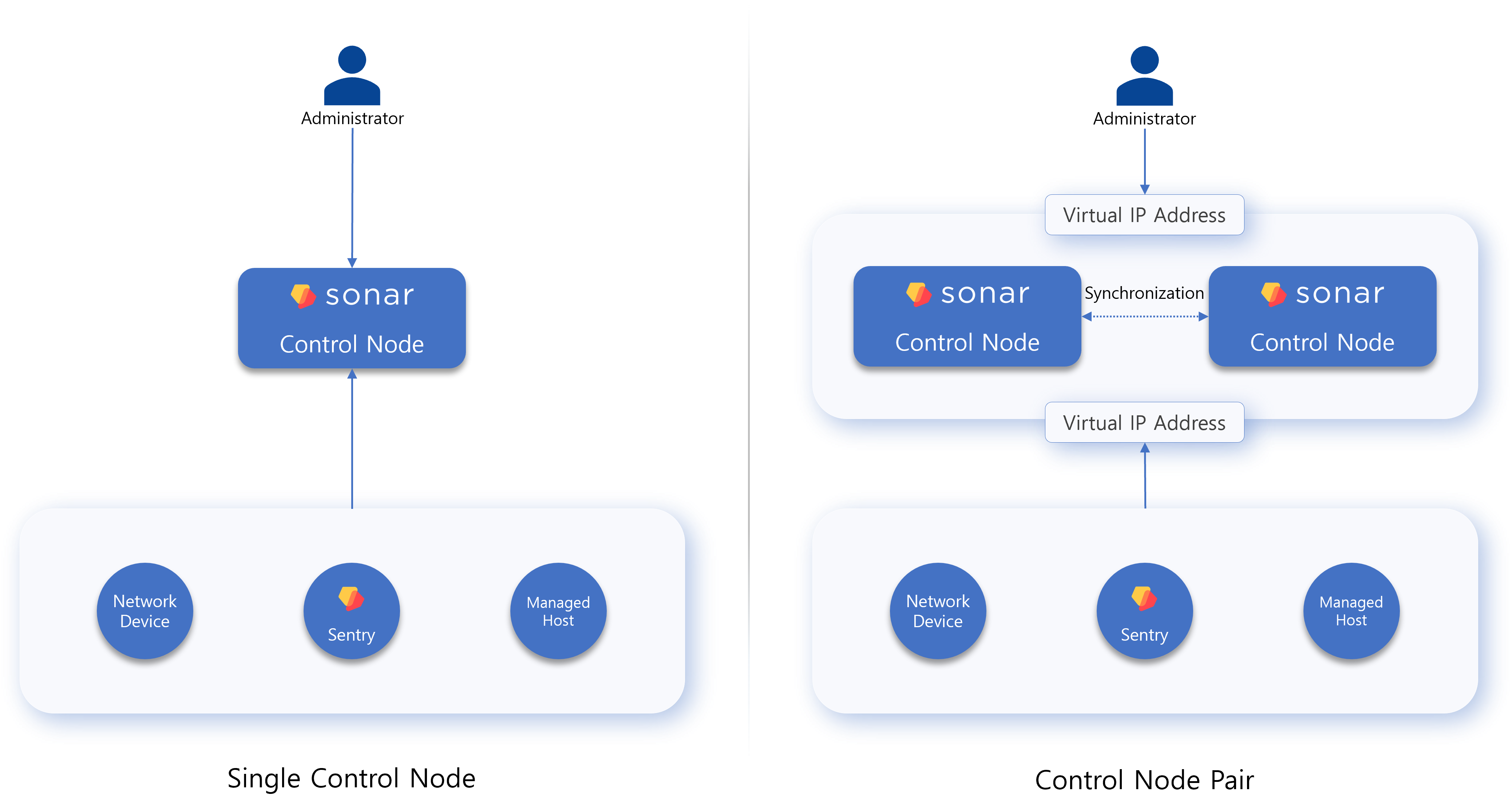
ログプレッソのクラスターは、構成する層に応じて以下のように分類されます。

* **1層**: コントロールノードのみで構成される層
* **2層**: フォワーダーノード - コントロールノード
* **2層（レガシー）**: データノード - コントロールノード
* **3層**: フォワーダーノード - データノード - コントロールノード

日々収集するオリジナルログの量に応じて、適切な層構成を選択できます。ログプレッソでは**3層アーキテクチャを推奨**しています。

1層：コントロールノード層

1層構成は以下のように示されます。左側は単一のコントロールノード、右側はコントロールノードのペアです。ログプレッソのリファレンスハードウェア基準で、1日あたり最大200GBのデータ処理が可能です。



**単一コントロールノード**

収集するデータ量が少ない場合、**単一サーバー**でデータノードとコントロールノードの両方の役割を兼任できます。ただし、ノード障害時にはデータ損失が発生する可能性があります。

**コントロールノードペア**

これは、障害発生時にもサービス継続性を確保するために、2台のコントロールノードを冗長構成で配置したTier-1高可用性（HA）構成です。

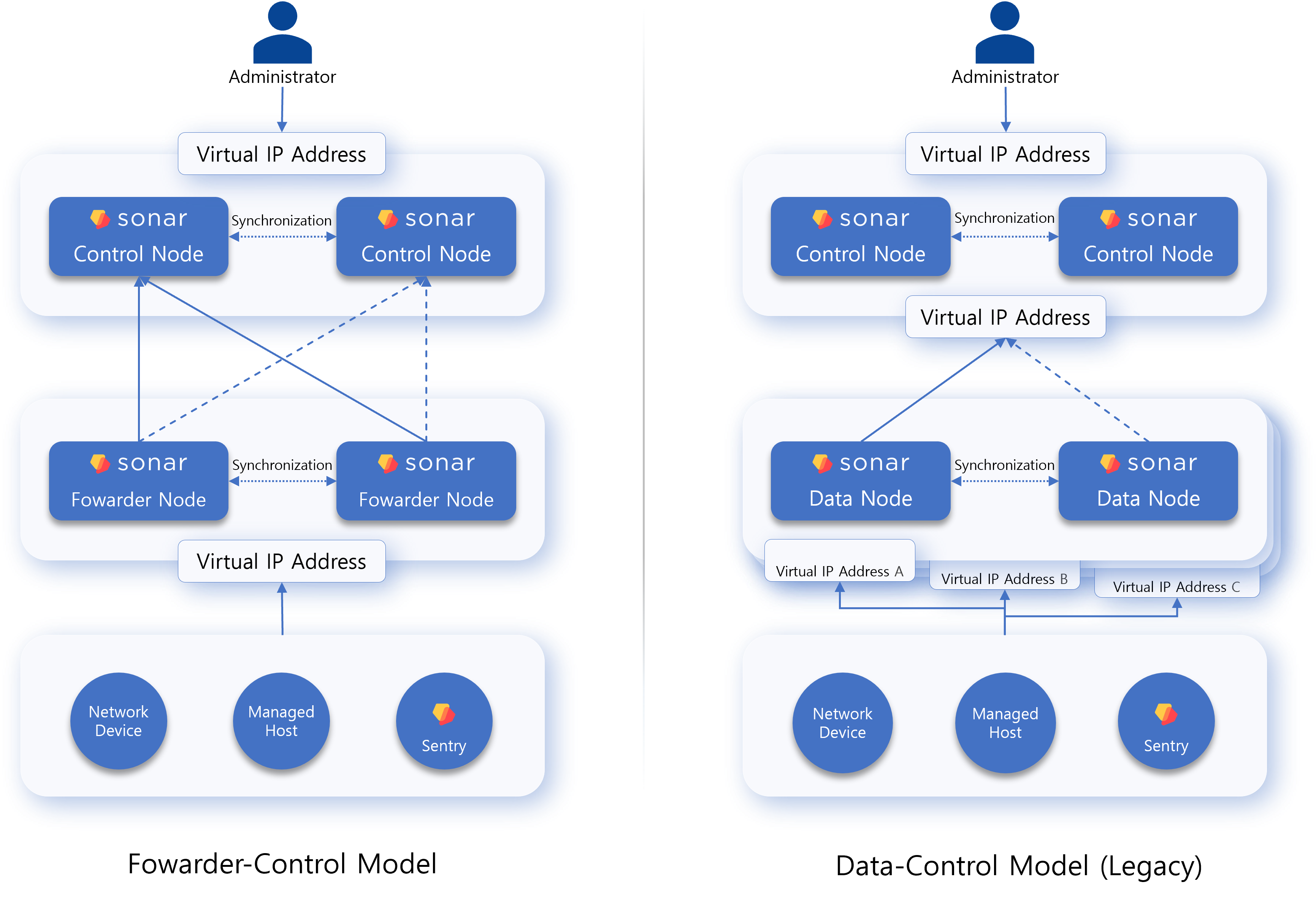
**各ノードは仮想IPアドレスを共有**しており、外部システムは仮想IPまたはコントロールノードに紐づくドメイン名でクラスターにアクセスできます。

* ネットワーク機器、管理対象ホスト、セントリーからデータが送信される場合、アクティブノードがデータを受信します。
* 管理者がシステムにアクセスする場合、アクティブノードがWebコンソールへのアクセスを提供します。

コントロールノードペアは水平スケールができないため、収集データ量が増加した場合は3層構成への移行を推奨します。

2層：フォワーダー-コントロール／データ-コントロール（レガシー）

2層構成は、データを収集するノードと保存するノードを分離します。下図の左側がフォワーダー-コントロールモデル、右側がデータ-コントロールモデル（レガシー）です。



**フォワーダー-コントロールモデル**

コントロールノードで構成された1層アーキテクチャに、フォワーダーノードのペアを追加した拡張構成であり、[ログプレッソ・クラウド](https://logpresso.cloud/)で基本的に採用されています。フォワーダーノードはバージョン4.0.2404.0から導入され、データゲートウェイおよびロードバランサーとして機能します（[関連ドキュメント](https://docs.logpresso.comnull)）。フォワーダーおよびコントロールノードは、可用性のために冗長構成を推奨します。

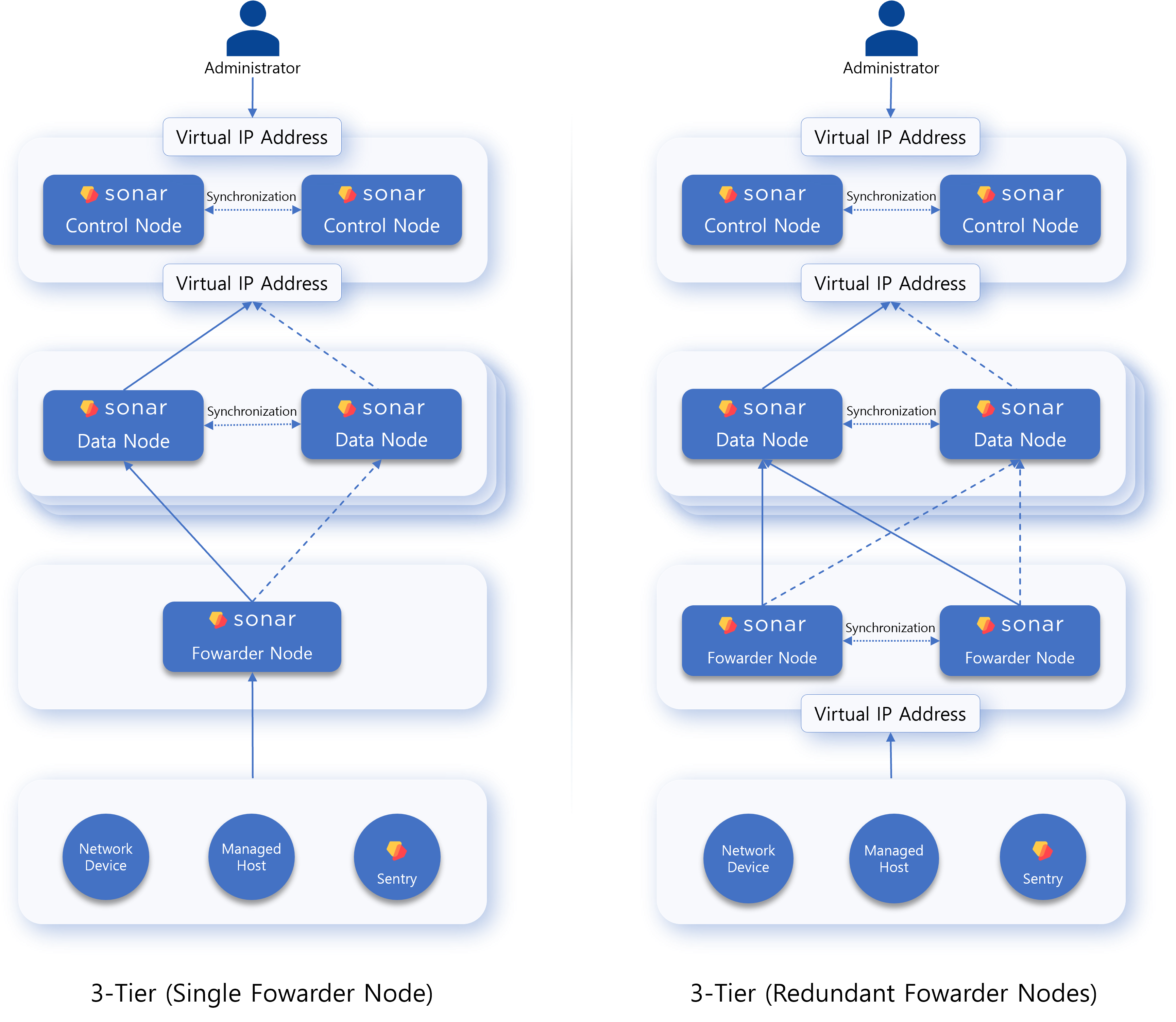
フォワーダーノードは下流ノードの水平スケールを考慮して使用され、この構成は3層アーキテクチャへの移行段階となります。コントロールノードは1ペアのみ利用可能なため、水平スケールには全体を3層構成へ変更する必要があります。

**データ-コントロールモデル（レガシー）**

バージョン4.0.2404.0以前に使用されていた構成で、1層構成にデータノードのペアを追加します。データ収集と分析を行う層を分離することで、データノードペア単位での水平スケールが可能となり、収集データ量が増加しても柔軟に対応できます。ただし、各データソース（ネットワーク機器、管理対象ホスト、セントリー）は指定されたデータノードペアと通信する必要があるため、データノードペアが増えるほどネットワーク構成が複雑になり、推奨されません。

3層：フォワーダー-データ-コントロール（推奨構成）

3層のフォワーダー-データ-コントロールモデルは、2層データ-コントロールモデル（レガシー）を置き換える新しいアーキテクチャであり、大規模データ収集環境における推奨クラスター構成です。



3層構成は2層構成のすべての欠点を解消します。データノードペアが2つ以上ある場合、必ずフォワーダーノードを構成する必要があります。フォワーダーノードは、2層データ-コントロールモデルで発生するトポロジーの問題を解決します。

レガシーから3層アーキテクチャへの移行

レガシーアーキテクチャから3層アーキテクチャへ移行するには、以下の手順を実施します。

フォワーダーノードの設置: 運用環境にフォワーダーノードを導入し、インストールします。

アプリの再インストール: フォワーダーノードにはアプリがインストールされていないため、必要に応じて[アプリ再インストール](https://docs.logpresso.comnull)を通じてフォワーダーサーバーにインストールします。

ロガーの置き換え: [ロガーの収集方式](https://docs.logpresso.comnull)に応じて異なるアプローチが必要です。**パッシブロガー**: 新規ロガーを構成し、レガシーロガーを停止・削除します。

収集先をフォワーダーノードペア、ロード先をデータノードペアとしてロガーを構成します。

データ送信元の送信先をフォワーダーノードの仮想IPまたはドメインアドレスに変更し、収集状況を確認します。

問題がなければ、レガシーロガーを停止または削除します。**アクティブロガー**: レガシーロガーを停止し、新規ロガーを構成します。

データノード上で稼働中のレガシーロガーを停止します。

収集先をフォワーダーノードペア、ロード先をデータノードペアとしてロガーを構成し、収集状況を確認します。

問題がなければ、必要に応じてレガシーロガーを削除します。

ノードタイプ

ログプレッソのクラスターは、コントロールノード、データノード、フォワーダーノードで構成されます。スタンドアロンのログプレッソ・ソナーサーバーは、データノードとコントロールノードの両方の役割を兼任します。

コントロールノード

コントロールノードは、ログプレッソクラスター内のすべてのノードを管理し、ユーザーがクラスターにアクセスするためのWebコンソールを提供します。冗長構成のコントロールノードは仮想IPアドレスを共有します。

**ノード制御**

フォワーダーおよびデータノードは、コントロールノードの仮想IPアドレスを利用して設定やポリシーの同期を要求し、コントロールノードは各ノードとポーリング方式で通信し、要求に応じて変更された設定やポリシーを送信します。

**ユーザーWebインターフェース**

ユーザーもコントロールノードの仮想IPまたはドメインアドレスを利用してWebコンソールにアクセスできます。ポリシー違反による弁明要求を受けた従業員や、弁明を審査する承認者もこの仮想IPアドレスを利用します。

**データ分析およびセキュリティ脅威・異常の検出**

コントロールノードは、[ストリームルール](https://docs.logpresso.comnull)や[バッチルール](https://docs.logpresso.comnull)シナリオに基づき、データノードにロードされたデータに対して以下のようなアクションを実行します。

* セキュリティ脅威や異常[イベント](https://docs.logpresso.comnull)の検出
* [チケット](https://docs.logpresso.comnull)の発行・管理
* [弁明要求](https://docs.logpresso.comnull)および承認管理
* 検出された脅威への[自動対応](https://docs.logpresso.comnull)

コントロールノードやクラスター内で定期的に実行されるほとんどのログプレッソクエリは、データノードからデータを読み取り・処理します。コントロールノードはクエリの実行計画を立て、各ノードから分散された結果を受け取ってデータを処理します。

コントロールノードはオンプレミス環境ではMariaDB、クラウド環境ではマネージドデータベースを使用します。

データノード

データノードは、ロガーで収集したデータを[テーブル](https://docs.logpresso.comnull)にパース、正規化、インデックス化、保存します。

**データロードとクエリ実行**

[パーサー](https://docs.logpresso.comnull)によるオリジナルデータのパースや、[ロガーモデル](https://docs.logpresso.comnull)で定義された正規化はすべてデータノードで実行されます。

すべてのデータノードは、オリジナルデータと正規化データを同名のテーブルに保存します。コントロールノードでログプレッソクエリが実行されると、[table](https://docs.logpresso.comnull)や[fulltext](https://docs.logpresso.comnull)などのデータ取得コマンドは各データノードで並列処理されます。

ライフサイクル管理: データノードは、テーブルで定義された[保存期間](https://docs.logpresso.comnull)や[データライフサイクル](https://docs.logpresso.comnull)に従ってデータを管理します。

フォワーダーノード

フォワーダーノードはバージョン4.0.2404.0で導入されました（[関連ドキュメント](https://docs.logpresso.comnull)）。冗長構成のフォワーダーノードもコントロールノード同様に仮想IPアドレスを共有します。

- データノードペアが2つ以上ある場合は、フォワーダーノードの構成を推奨します。- データノードペアをアクティブ-アクティブで運用するには、L4スイッチまたはネットワークロードバランサーが必要です。

**データゲートウェイ**

[ロガー](https://docs.logpresso.comnull)はフォワーダーノード上で稼働し、ログプレッソクラスターのデータ送信ゲートウェイとして機能します。フォワーダーノードの仮想IPまたはドメインアドレスがゲートウェイアドレスとして利用されます。

データノードもフォワーダーノードの代わりにデータゲートウェイの役割を担うことは可能ですが、推奨されません。データノードペアが増えるごとにデータゲートウェイの数も増加し、データ送信元はそのうち1つのみを指定する必要があるため、ネットワーク構成が複雑になります。

**ロードバランシング**

フォワーダーノードで受信・収集したデータはデータノードに転送されます。フォワーダーノードは[ロガー](https://docs.logpresso.comnull)で定義された送信方式に従い、複数のデータノードペアにデータを均等に分散するロードバランシングを行うか、特定のノードペアにデータを送信します。

フォワーダーノードがデータノードとの通信障害を検知した場合、送信すべきデータを一時的にメモリおよびローカルディスクに保存し、障害復旧後に保存データをデータノードへ再送信します。送信完了後、ローカルストレージ上のデータは削除されます。

構成順序

クラスターを構成する際は、以下の順序でノードをセットアップしてください。

コントロールノードおよび冗長構成

データノードおよび冗長構成

フォワーダーノードおよび冗長構成

本ドキュメントではWebコンソールの利用方法のみを扱い、実際のインストール手順は別ドキュメントで提供します。

* コントロールノードおよびデータノードのインストール手順は別途提供します。
* フォワーダーノードのインストールおよび構成手順については、[こちらのドキュメント](https://docs.logpresso.comnull)をご参照ください。

データライフサイクル

データライフサイクルとは、一般的にデータの生成から削除までの一連のプロセスを指します。ログプレッソ・ソナーは、ログやPCAPファイルなどの時系列で生成されるデータを収集します。これらのデータは、「現在」に近いほど重要度が高いという特徴があります。

保存データ量が増加するほど、ストレージコストも増加します。ストレージライフサイクル機能を利用することで、頻繁にアクセスされる最新データは高速だが高価なストレージに、アクセス頻度の低い古いデータは低速だが安価なストレージに保存し、パフォーマンスとコストのバランスを取ることができます。

保存場所が変更された場合や変更中であっても、データの検索・分析機能は単一ストレージ利用時と同様に動作するため、システム運用や利用に影響はありません。

データライフサイクルは収集データのみに適用され、クラスターを構成するノードのシステムデータには適用されません。

ストレージ層

ログプレッソ・ソナーはストレージ階層化（ティアリング）をサポートしており、頻繁にアクセスされる最新データは最高性能のストレージ（SSD）に、アクセス頻度の低い古いデータは比較的低性能で安価なストレージ（NAS、クラウドオブジェクトストレージ）に保存されます。

ログプレッソ・ソナーのストレージは3つの層で構成されます。

|  |  |  |  |
| --- | --- | --- | --- |
| 区分 | Hot（Tier 1） | Warm（Tier 2） | Cold（Tier 3） |
| デバイスタイプ | NVMe、SSD | HDD、WORM | WORM、NAS、クラウドオブジェクトストレージ |
| 検索性能 | 非常に高い | 普通 | 低い |
| 統計処理性能 | 高い | 普通 | 低い |
| レプリケーション数 | 2 | 2 | 1 |
| 単価 | 高い | 普通 | 低い |
| 構成目的 | 検索性能の最大化 | 一般的な分析 | データアーカイブ、コンプライアンス対応 |

**Hot**

収集データを最初に保存する最上位層で、高コスト・高性能ストレージを利用します。設定期間経過後、下位層（WarmまたはCold）へロールオーバーされます。

**Warm**

**Hot**層からロールオーバーされたデータを保持する、中間コスト・中間性能のストレージです。ノードが冗長構成の場合、**ノードAとノードBがそれぞれロールオーバー**を実行し、各データが1回複製されます。

**Cold**

**Hot**および**Warm**層からロールオーバーされたデータを保持する、低コスト・低性能のストレージです。ノードが冗長構成でも、**データは1回のみロールオーバー**されます。

**Cold**層は、主にコンプライアンス対応のために長期間保存が必要な古いデータや、利用頻度が極めて低いデータの保存に利用されます。

運用環境や目的に応じて、**Warm**層や**Cold**層は選択的に適用できます。WORMストレージを利用する場合は、ログプレッソストアからWORMドライバーを取得してください。

WarmおよびColdディレクトリでNFSを利用する場合は、十分なデータ転送速度が保証されていることを確認してください。

ロールオーバー

ロールオーバーとは、保存期間や容量に基づいてデータを下位層へ移動する操作です。例えば、**Hot**、**Warm**、**Cold**各層に120日ずつ保存期間を設定した場合、合計360日間各層でデータが保持されます。**Cold**層で保存期間を超えたデータは、設定に応じて削除または永久アーカイブされます。



* ロールオーバーは収集データに適用され、システムデータは常に**Hot**層に保持されます。
* ストレージ層間のデータ転送速度や実行スケジュールは、[ロールオーバー設定](https://docs.logpresso.comnull)で制限できます。
* [最大ストレージ容量](https://docs.logpresso.comnull)を指定できます。各ノードは15分ごとに最大容量をチェックし、超過分は下位層へロールオーバーされます。

ログプレッソ・ソナーはロールオーバー時のデータ損失を防ぐため、以下のように動作します。

下位層へ送信するファイルを一時ファイルとして複製します。

複製が完了したら、上位ストレージからファイルを削除し、一時ファイルを元のファイル名にリネームします。

下位層ストレージがWORMまたはクラウドストレージの場合、一時ファイル複製なしでファイル転送を構成できます。

既存機能との違い

データライフサイクルは、[テーブルの保存期間](https://docs.logpresso.comnull)や[ノードのストレージ管理](https://docs.logpresso.comnull)と類似していますが、以下のような違いがあります。

|  |  |  |
| --- | --- | --- |
| 区分 | テーブル保存期間（ローカル設定） | ライフサイクル（グローバル設定） |
| 適用範囲 | 個別テーブル内のデータ | ストレージ全体のすべての記録データ |
| 管理対象 | テーブルパーティション単位のデータ | テーブルパーティション単位のデータ |
| 保存期間満了時の動作 | データ削除 | 下位ストレージ層へのロールオーバー |
| ストレージ管理 | 古いデータの削除または収集停止 | （1次）ロールオーバー、（2次）削除またはアーカイブ |

データライフサイクルとテーブル保存期間は独立して動作します。指定した保存期間のうち短い方が適用されるため、以下のいずれかの方法でデータ管理を行ってください。

データライフサイクルのみを利用

* テーブル作成時の保存期間を「永久保存（デフォルト）」のままにします。
* ライフサイクルによる管理はグローバル設定のため、テーブル単位よりも容易です。

データライフサイクルを主機能、テーブル保存期間を補助機能として利用

* データライフサイクルの保存期間をグローバル設定します。
* 必要な場合のみ、テーブル保存期間をグローバル設定より短く設定します。

ライフサイクルの初期値

初期値はデフォルトで設定されていません。この状態では、テーブルの保存期間およびノードのストレージ管理設定に従って動作します。

**テーブル**設定で定義された[保存期間](https://docs.logpresso.comnull)：保存期間を超えたデータを削除または永久アーカイブします。

**ノード**設定で定義された[ストレージ管理](https://docs.logpresso.comnull)：ローカルストレージが満杯になる前に古いデータを削除またはデータ収集を停止します。この場合、監視対象ストレージはログプレッソのデータ保存ディレクトリが存在するパーティションです。