OpenShift Container Platform 4.5

ロギング

OpenShift Container Platform でのクラスターロギングの設定

Last Updated: 2023-05-22

OpenShift Container Platform 4.5 ロギング

OpenShift Container Platform でのクラスターロギングの設定

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

本書では、クラスターロギング機能のインストール、設定および使用方法について説明します。クラスターロギングは、各種の OpenShift Container Platform サービスについてのログを集計します。

目次

第1章 クラスターロギングについて 6
1.1. クラスターロギングのデプロイについて 6
1.1.1. クラスターロギングのコンポーネントについて 6
1.1.2. ロギングコレクターについて 7
1.1.3. ログストアについて 7
1.1.4. ロギングの可視化について 8
1.1.5. イベントのルーティングについて 8
1.1.6. ログ転送 9

第2章 クラスターロギングのインストール 10
2.1. WEB コンソールを使用したクラスターロギングのインストール 10
2.2. インストール後のタスク 15
2.3. CLI を使用したクラスターロギングのインストール 15
2.4. インストール後のタスク 23
2.4.1. Kibana インデックスパターンの定義 23
2.4.2. ネットワークの分離が有効にされている場合のプロジェクト間のトラフィックの許可 24

第3章 クラスターロギングデプロイメントの設定 26
3.1. クラスターロギングカスタムリソースについて 26
3.1.1. ClusterLogging カスタムリソースについて 26
3.2. ロギングコレクターの設定 27
3.2.1. サポートされる設定 27
3.2.2. ロギングコレクター Pod の表示 28
3.2.3. ログコレクター CPU およびメモリー制限の設定 28
3.2.4. ロギングコレクターのアラートについて 29
3.2.5. デフォルトの Elasticsearch ログストアを使用しない場合の未使用のコンポーネントの削除 29
3.3. ログストアの設定 31
3.3.1. 監査ログのログストアへの転送 31
3.3.2. ログ保持時間の設定 34
3.3.3. ログストアの CPU およびメモリー要求の設定 36
3.3.4. ログストアのレプリケーションポリシーの設定 37
3.3.5. Elasticsearch Pod のスケールダウン 38
3.3.6. ログストアの永続ストレージの設定 39
3.3.7. emptyDir ストレージのログストアの設定 40
3.3.8. Elasticsearch クラスターのローリング再起動の実行 40
3.3.9. ログストアサービスのルートとしての公開 43
3.4. ログビジュアライザーの設定 46
3.4.1. CPU およびメモリー制限の設定 46
3.4.2. ログビジュアライザーノードの冗長性のスケーリング 48
3.4.3. 容認を使用したログビジュアライザー Pod の配置の制御 48
3.5. クラスターロギングストレージの設定 49
3.5.1. クラスターロギングおよび OpenShift Container Platform のストレージについての考慮事項 49
3.5.2. 追加リソース 50
3.6. クラスターロギングコンポーネントの CPU およびメモリー制限の設定 50
3.6.1. CPU およびメモリー制限の設定 50
3.7. 容認を使用した クラスターロギング POD 配置の制御 52
3.7.1. 容認を使用したログストア Pod の配置の制御 53
3.7.2. 容認を使用したログビジュアライザー Pod の配置の制御 54
3.7.3. 容認を使用したログコレクター Pod 配置の制御 55
3.7.4. 追加リソース 56
3.8. ノードセレクターを使用したクラスターロギングリソースの移動 56

3.8.1. クラスターロギングリソースの移動 57
3.9. SYSTEMD-JOURNALD および FLUENTD の設定 60
3.9.1. クラスターロギング用の systemd-journald の設定 60
3.10. ログキュレーターの設定 63
3.10.1. Curator スケジュールの設定 63
3.10.2. Curator インデックス削除の設定 64
3.11. メンテナーンスとサポート 66
3.11.1. サポートされる設定 66
3.11.2. サポートされない設定 67
3.11.3. 管理外の Operator のサポートポリシー 67

第4章 リソースのログの表示 69
4.1. リソースログの表示 69

第5章 KIBANA を使用したクラスターログの表示 71
5.1. KIBANA インデックスパターンの定義 71
5.2. KIBANA を使用したクラスターログの表示 72

第6章 ログのサードパーティーシステムへの転送 75
6.1. FLUENTD 転送プロトコルを使用したログの転送 75
6.2. SYSLOG プロトコルを使用したログの転送 79
6.3. ログ転送 API を使用したログの転送 82
6.3.1. ログ転送 API について 83
外部ログアグリゲーターが利用できない場合の Fluentd のログの処理 85
6.3.2. ログ転送 API の有効化 86
6.3.3. ログ転送 API を使用したログ転送の設定 86
6.3.3.1. ログ転送カスタムリソースのサンプル 88
6.3.4. ログ転送 API の無効化 89

第7章 KUBERNETES イベントの収集および保存 91
7.1. イベントルーターのデプロイおよび設定 91

第8章 クラスターロギングの更新 95
8.1. クラスターロギングの更新 95
8.1.1. 更新後のタスク 100
8.2. KIBANA インデックスパターンの定義 100

第9章 クラスターロギングのトラブルシューティング 102
9.1. クラスターロギングのステータス表示 102
9.1.1. Cluster Logging Operator のステータス表示 102
9.1.1.1. 状態メッセージ (condition message) のサンプル 104
9.1.2. クラスターロギングコンポーネントのステータスの表示 106
9.2. ログストアのステータスの表示 107
9.2.1. ログストアのステータスの表示 107
9.2.1.1. 状態メッセージ (condition message) のサンプル 109
9.2.2. ログストアコンポーネントのステータスの表示 111
9.3. クラスターロギングのアラートについて 114
9.3.1. ロギングコレクターアラートの表示 114
9.3.2. ロギングコレクターのアラートについて 115
9.3.3. Elasticsearch アラートルール 115
9.4. ログキュレーターのトラブルシューティング 116
9.4.1. ログ収集のトラブルシューティング 116
9.5. RED HAT サポート用のロギングデータの収集 117
9.5.1. must-gather ツールについて 118
9.5.2. 前提条件 118

9.5.3. クラスターロギングデータの収集 118

第10章 クラスターロギングのアンインストール 120
10.1. OPENSHIFT CONTAINER PLATFORM からのクラスターロギングのアンインストール 120

第11章 エクスポートされるフィールド 122
11.1. デフォルトのエクスポートされるフィールド 122
最上位フィールド 122
collectd フィールド 124
collectd.processes フィールド 125
collectd.processes.ps_disk_ops フィールド 125
collectd.processes.ps_cputime フィールド 125
collectd.processes.ps_count フィールド 126
collectd.processes.ps_pagefaults フィールド 126
collectd.processes.ps_disk_octets フィールド 126
collectd.disk フィールド 127
collectd.disk.disk_merged フィールド 127
collectd.disk.disk_octets フィールド 127
collectd.disk.disk_time フィールド 127
collectd.disk.disk_ops フィールド 128
collectd.disk.disk_io_time フィールド 128
collectd.interface フィールド 128
collectd.interface.if_octets フィールド 128
collectd.interface.if_packets フィールド 128
collectd.interface.if_errors フィールド 129
collectd.interface.if_dropped フィールド 129
collectd.virt フィールド 129
collectd.virt.if_octets フィールド 129
collectd.virt.if_packets フィールド 130
collectd.virt.if_errors フィールド 130
collectd.virt.if_dropped フィールド 130
collectd.virt.disk_ops フィールド 130
collectd.virt.disk_octets フィールド 131
collectd.CPU フィールド 131
collectd.df フィールド 131
collectd.entropy フィールド 132
collectd.memory フィールド 132
collectd.swap フィールド 132
collectd.load フィールド 132
collectd.load.load フィールド 133
collectd.aggregation フィールド 133
collectd.statsd フィールド 133
collectd.postgresql フィールド 136
11.2. SYSTEMD のエクスポートされるフィールド 137
systemd.k フィールド 137
systemd.t フィールド 138
systemd.u フィールド 139
11.3. KUBERNETES のエクスポートされるフィールド 140
kubernetes.labels フィールド 140
kubernetes.annotations フィールド 141
11.4. コンテナーのエクスポートされるフィールド 141
pipeline_metadata.collector フィールド 141
pipeline_metadata.normalizer フィールド 141

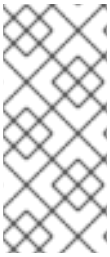
11.5. OVIRT のエクスポートされるフィールド 142
ovirt.engine フィールド 142
11.6. AUSHAPE のエクスポートされるフィールド 142
aushape.data フィールド 143
11.7. TLOG のエクスポートされるフィールド 143

第1章 クラスターロギングについて

クラスター管理者は、クラスターロギングをデプロイし、ノードシステムの監査ログ、アプリケーションコンテナーログ、およびインフラストラクチャーログなどの OpenShift Container Platform クラスターからのすべてのログを集計できます。クラスターロギングはクラスター全体でこれらのログを集計し、それらをデフォルトのログストアに保存します。Kibana Web コンソールを使用して、ログデータを可視化 できます。

クラスターロギングは以下のタイプのログを集計します。

- **application**: クラスターで実行される、インフラストラクチャーコンテナーアプリケーションを除くユーザーアプリケーションによって生成されるコンテナーログ。
- **infrastructure**: ジャーナルログなどの、クラスターで実行されるインフラストラクチャーコンポーネントおよび OpenShift Container Platform ノードで生成されるログ。インフラストラクチャーコンポーネントは、**openshift***、 **kube***、または **default** プロジェクトで実行される Pod です。
- **audit**: ノード監査システム (auditd) で生成されるログ (**/var/log/audit/audit.log** ファイルに保存される)、および Kubernetes apiserver および OpenShift apiserver の監査ログ。



注記

内部 OpenShift Container Platform Elasticsearch ログストアは監査ログのセキュアなストレージを提供しないため、デフォルトで監査ログは内部 Elasticsearch インスタンスに保存されません。監査ログを内部ログストアに送信する必要がある場合 (Kibana で監査ログを表示するなど)、Forward audit logs to the log store で説明されているようにログ転送 API を使用する必要があります。

1.1. クラスターロギングのデプロイについて

OpenShift Container Platform クラスター管理者は、OpenShift Container Platform Web コンソールまたは CLI コマンドを使用してクラスターロギングをデプロイし、Elasticsearch Operator および Cluster Logging Operator をインストールできます。Operator がインストールされている場合、**ClusterLogging** カスタムリソース (Custom Resource、CR) を作成してクラスターロギング Pod およびクラスターロギングのサポートに必要な他のリソースをスケジュールします。Operator はクラスターロギングのデプロイ、アップグレード、および維持を行います。

ClusterLogging CR は、ログを収集し、保存し、視覚化するために必要なロギングスタックのすべてのコンポーネントを含む完全なクラスターロギング環境を定義します。Cluster Logging Operator は Cluster Logging CR を監視し、ロギングデプロイメントを適宜調整します。

管理者およびアプリケーション開発者は、表示アクセスのあるプロジェクトのログを表示できます。

詳細は、ログコレクターの設定 について参照してください。

1.1.1. クラスターロギングのコンポーネントについて

クラスターロギングコンポーネントには、すべてのノードおよびコンテナーログを収集し、それらをログストアに書き込む OpenShift Container Platform クラスターの各ノードにデプロイされるコレクターが含まれます。一元化された Web UI を使用し、集計されたデータを使用して高度な可視化 (visualization) およびダッシュボードを作成できます。

クラスターロギングの主要コンポーネントは以下の通りです。

- collection: これは、クラスターからログを収集し、それらをフォーマットし、ログストアに転送するコンポーネントです。現在の実装は Fluentd です。
- log store: これはログが保存される場所です。デフォルトの実装は Elasticsearch です。デフォルトの Elasticsearch ログストアを使用するか、またはログを外部ログストアに転送することができます。デフォルトのログストアは、短期の保存について最適化され、テストされています。
- visualization: これは、ログ、グラフ、チャートなどを表示するために使用される UI コンポーネントです。現在の実装は Kibana です。

本書では、特筆されない限り、log store と Elasticsearch、visualization と Kibana、collection と Fluentd を区別せずに使用する場合があります。

1.1.2. ロギングコレクターについて

OpenShift Container Platform は Fluentd を使用してコンテナーおよびノードのログを収集します。

デフォルトでは、ログコレクターは以下のソースを使用します。

- すべてのシステムログ用の journald
- すべてのコンテナーログ用の **/var/log/containers/*.log**

ロギングコレクターは、Pod を各 OpenShift Container Platform ノードにデプロイするデーモンセットとしてデプロイされます。システムおよびインフラストラクチャーのログは、オペレーティングシステム、コンテナーランタイム、および OpenShift Container Platform からの journald ログメッセージによって生成されます。アプリケーションログは CRI-O コンテナーエンジンによって生成されます。Fluentd はこれらのソースからログを収集し、OpenShift Container Platform で設定したように内部または外部に転送します。

コンテナーランタイムは、プロジェクト、Pod 名、およびコンテナー ID などのログメッセージのソースを特定するための最小限の情報を提供します。この情報だけでは、ログのソースを一意に特定することはできません。ログコレクターがログを処理する前に、指定された名前およびプロジェクトを持つ Pod が削除される場合、ラベルやアノテーションなどの API サーバーからの情報は利用できない可能性があります。そのため、似たような名前の Pod やプロジェクトからログメッセージを区別したり、ログのソースを追跡することができない場合があります。この制限により、ログの収集および正規化は **ベストエフォート** ベースであると見なされます。

重要

利用可能なコンテナーランタイムは、ログメッセージのソースを特定するための最小限の情報を提供し、個別のログメッセージが一意となる確証はなく、これらのメッセージにより、そのソースを追跡できる訳ではありません。

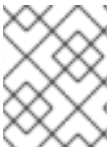
詳細は、ログコレクターの設定 について参照してください。

1.1.3. ログストアについて

デフォルトで、OpenShift Container Platform は Elasticsearch (ES) を使用してログデータを保存します。オプションで、ログ転送機能を使用して、Fluentd プロトコル、syslog プロトコル、または OpenShift Container Platform ログ転送 API を使用してログを外部ログストアに転送できます。

クラスターロギング Elasticsearch インスタンスは、短期 (約 7 日間) の保存について最適化され、テストされています。長期間ログを保持する必要がある場合は、データをサードパーティーのストレージシステムに移動することが推奨されます。

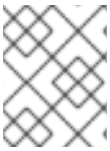
Elasticsearch は Fluentd からのログデータをデータストアまたは **インデックス** に編成し、それぞれのインデックスを **シャード** と呼ばれる複数の部分に分割します。これは、Elasticsearch クラスターの Elasticsearch ノードセット全体に分散されます。Elasticsearch を、**レプリカ** と呼ばれるシャードのコピーを作成するように設定できます。Elasticsearch はこれを Elasticsearch ノード全体に分散します。**ClusterLogging** カスタムリソース (CR) により、データの冗長性および耐障害性を確保するためにシャードを複製する方法を指定できます。また、**ClusterLogging** CR の保持ポリシーを使用して各種のログが保持される期間を指定することもできます。



注記

インデックステンプレートのプライマリーシャードの数は Elasticsearch データノードの数と等しくなります。

Cluster Logging Operator および Elasticsearch Operator は、各 Elasticsearch ノードが独自のストレージボリュームを含む一意のデプロイメントを使用してデプロイされるようにします。**ClusterLogging** カスタムリソース (CR) を使用して Elasticsearch ノードの数を適宜増やすことができます。ストレージの設定に関する考慮事項については、Elasticsearch ドキュメント を参照してください。



注記

可用性の高い Elasticsearch 環境には 3 つ以上の Elasticsearch ノードが必要で、それぞれが別のホストに置かれる必要があります。

Elasticsearch インデックスに適用されているロールベースアクセス制御 (RBAC) は、開発者のログの制御アクセスを可能にします。管理者はすべてのログに、開発者は各自のプロジェクトのログにのみアクセスできます。

詳細は、ログストアの設定 について参照してください。

1.1.4. ロギングの可視化について

OpenShift Container Platform は Kibana を使用して、Fluentd によって収集され、Elasticsearch によってインデックス化されるログデータを表示します。

Kibana は、ヒストグラム、線グラフ、円グラフその他の可視化機能を使用して Elasticsearch データをクエリーし、検出し、可視化するためのブラウザーベースのコンソールインターフェイスです。

詳細は、ログビジュアライザーの設定 について参照してください。

1.1.5. イベントのルーティングについて

イベントルーターは、クラスターロギングで収集できるように OpenShift Container Platform イベントを監視する Pod です。イベントルーターはすべてのプロジェクトからイベントを収集し、それらを **STDOUT** に書き込みます。Fluentd はそれらのイベントを収集し、それらを OpenShift Container Platform Elasticsearch インスタンスに転送します。Elasticsearch はイベントを **infra** インデックスにインデックス化します。

イベントルーターは手動でデプロイする必要があります。

詳細は、 Kubernetes イベントの収集および保存 について参照してください。

1.1.6. ログ転送

デフォルトで、OpenShift Container Platform クラスターロギングは **ClusterLogging** カスタムリソース (CR) に定義されるデフォルトの内部 Elasticsearch ログストアにログを送信します。ログを他のログアグリゲーターに転送する必要がある場合、ログ転送機能を使用してログをクラスター内外の特定のエンドポイントに送信することができます。

詳細は、ログのサードパーティーシステムへの転送 について参照してください。

第2章 クラスターロギングのインストール

クラスターロギングは、Elasticsearch および Cluster Logging Operator をデプロイしてインストールできます。Elasticsearch Operator は、クラスターロギングによって使用される Elasticsearch クラスターを作成し、管理します。Cluster Logging Operator はロギングスタックのコンポーネントを作成し、管理します。

クラスターロギングを OpenShift Container Platform にデプロイするプロセスには以下が関係します。

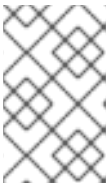
- cluster logging storage considerations を確認します。
- OpenShift Container Platform Web コンソール、または CLI を使用した Elasticsearch Operator および Cluster Logging Operator のインストール

2.1. WEB コンソールを使用したクラスターロギングのインストール

OpenShift Container Platform Web コンソールを使って Elasticsearch および Cluster Logging Operator をインストールすることができます。

前提条件

- Elasticsearch の必要な永続ストレージがあることを確認します。各 Elasticsearch ノードには独自のストレージボリュームが必要であることに注意してください。



注記

永続ストレージにローカルボリュームを使用する場合は、**LocalVolume** オブジェクトの **volumeMode: block** で記述される raw ブロックボリュームを使用しないでください。Elasticsearch は raw ブロックボリュームを使用できません。

Elasticsearch はメモリー集約型アプリケーションです。デフォルトで、OpenShift Container Platform はメモリー要求および 16 GB の制限を持つ 3 つの Elasticsearch ノードをインストールします。OpenShift Container Platform ノードの最初の 3 つのセットには、Elasticsearch をクラスター内で実行するのに十分なメモリーがない可能性があります。Elasticsearch に関連するメモリーの問題が発生した場合、既存ノードのメモリーを増やすのではなく、Elasticsearch ノードをクラスターにさらに追加します。

手順

OpenShift Container Platform Web コンソールを使って Elasticsearch Operator および Cluster Logging Operator をインストールするには、以下を実行します。

1. Elasticsearch Operator をインストールします。
   a. OpenShift Container Platform Web コンソールで、**Operators → OperatorHub** をクリックします。
   b. 利用可能な Operator の一覧から **Elasticsearch Operator** を選択し、**Install** をクリックします。
   c. **All namespaces on the cluster**が **Installation Mode** で選択されていることを確認します。
   d. **openshift-operators-redhat** が **Installed Namespace** で選択されていることを確認します。
   openshift-operators-redhat namespace を指定する必要があります。**openshift-**

operators namespace には信頼されていないコミュニティー Operator が含まれる可能性があり、OpenShift Container Platform メトリクスと同じ名前でメトリクスを公開する可能性があるため、これによって競合が生じる可能性があります。

e. **Enable operator recommended cluster monitoring on this namespace**を選択します。このオプションは、namespace オブジェクトに **openshift.io/cluster-monitoring: "true"** ラベルを設定します。クラスターモニターリングが **openshift-operators-redhat** namespace を収集できるように、このオプションを選択する必要があります。

f. **Update Channel** として **4.5** を選択します。

g. **Approval Strategy** を選択します。

- **Automatic** ストラテジーにより、Operator Lifecycle Manager (OLM) は新規バージョンが利用可能になると Operator を自動的に更新できます。
- **Manual** ストラテジーには、Operator の更新を承認するための適切な認証情報を持つユーザーが必要です。

h. **Install** をクリックします。

i. **Operators → Installed Operators** ページに切り替えて、Elasticsearch Operator がインストールされていることを確認します。

j. **Status** が **Succeeded** の状態で、**Elasticsearch Operator** が すべてのプロジェクトに一覧表示されていることを確認します。

2. Cluster Logging Operator をインストールします。

a. OpenShift Container Platform Web コンソールで、**Operators → OperatorHub** をクリックします。

b. 利用可能な Operator の一覧から **Cluster Logging** を選択し、**Install** をクリックします。

c. **A specific namespace on the cluster**が **Installation Mode** で選択されていることを確認します。

d. **Operator recommended namespace** が **Installed Namespace** で **openshift-logging** になっていることを確認します。

e. **Enable operator recommended cluster monitoring on this namespace**を選択します。このオプションは、namespace オブジェクトに **openshift.io/cluster-monitoring: "true"** ラベルを設定します。クラスターモニターリングが **openshift-logging** namespace を収集できるように、このオプションを選択する必要があります。

f. **Update Channel** として **4.5** を選択します。

g. **Approval Strategy** を選択します。

- **Automatic** ストラテジーにより、Operator Lifecycle Manager (OLM) は新規バージョンが利用可能になると Operator を自動的に更新できます。
- **Manual** ストラテジーには、Operator の更新を承認するための適切な認証情報を持つユーザーが必要です。

h. **Install** をクリックします。

i. **Operators → Installed Operators** ページに切り替えて、Cluster Logging Operator がインストールされていることを確認します。

j. **Cluster Logging** が **Status** が **Succeeded** の状態で **openshift-logging** プロジェクトに一覧表示されていることを確認します。
Operator がインストール済みとして表示されない場合に、さらにトラブルシューティングを実行します。

- **Operators → Installed Operators** ページに切り替え、**Status** 列でエラーまたは失敗の有無を確認します。
- **Workloads → Pods** ページに切り替え、 **openshift-logging** プロジェクトの Pod で問題を報告しているログの有無を確認します。

3. クラスターロギングのインスタンスを作成します。

a. **Administration → Custom Resource Definitions**ページに切り替えます。

b. **Custom Resource Definitions**ページで、**ClusterLogging** をクリックします。

c. **Custom Resource Definition Overview**ページで、**Actions** メニューから **View Instances** を選択します。

d. **ClusterLoggings** ページで、 **Create ClusterLogging** をクリックします。
データを読み込むためにページを更新する必要がある場合があります。

e. YAML フィールドで、コードを以下に置き換えます。

注記

このデフォルトのクラスターロギング設定は各種の環境をサポートすることが予想されます。クラスターロギングのクラスターに加えることのできる変更についての詳細は、クラスターロギングコンポーネントのチューニングおよび設定についてのトピックを確認してください。

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance" 1
  namespace: "openshift-logging"
spec:
  managementState: "Managed" 2
  logStore:
    type: "elasticsearch" 3
    retentionPolicy: 4
      application:
        maxAge: 1d
      infra:
        maxAge: 7d
      audit:
        maxAge: 7d
    elasticsearch:
      nodeCount: 3 5
      storage:
        storageClassName: "<storage-class-name>" 6
```

```
      size: 200G
    resources: 7
      requests:
        memory: "8Gi"
    proxy: 8
      resources:
        limits:
          memory: 256Mi
        requests:
          memory: 256Mi
    redundancyPolicy: "SingleRedundancy"
visualization:
  type: "kibana" 9
  kibana:
    replicas: 1
curation:
  type: "curator"
  curator:
    schedule: "30 3 * * *" 10
collection:
  logs:
    type: "fluentd" 11
    fluentd: {}
```

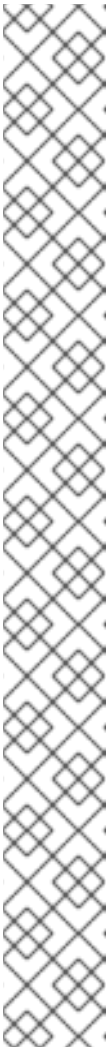
1. 名前は **instance** である必要があります。
2. クラスターロギングの管理状態。クラスターロギングのデフォルト値を変更する場合は、これを **Unmanaged** (管理外) に設定する必要がある場合があります。ただし、管理外のデプロイメントはクラスターロギングが管理対象の状態に戻されるまで更新を受信しません。
3. Elasticsearch の設定に必要な設定。CR を使用してシャードのレプリケーションポリシーおよび永続ストレージを設定できます。
4. Elasticsearch が各ログソースを保持する期間を指定します。整数および時間の指定 (weeks(w)、hour(h/H)、minutes(m)、および seconds(s)) を入力します。たとえば、7 日の場合は **7d** となります。**maxAge** よりも古いログは削除されます。各ログソースの保持ポリシーを指定する必要があります。そうしない場合、Elasticsearch インデックスはそのソースに対して作成されません。
5. Elasticsearch ノードの数を指定します。この一覧に続く注記を確認してください。
6. Elasticsearch ストレージの既存のストレージクラスの名前を入力します。最適なパフォーマンスを得るには、ブロックストレージを割り当てるストレージクラスを指定します。ストレージクラスを指定しない場合、OpenShift Container Platform は一時ストレージのみのクラスターロギングをデプロイします。
7. Elasticsearch ストレージの既存のストレージクラスの名前を入力します。最適なパフォーマンスを得るには、ブロックストレージを割り当てるストレージクラスを指定します。ストレージクラスを指定しない場合、OpenShift Container Platform は一時ストレージのみのクラスターロギングをデプロイします。
8. 必要に応じて CPU およびメモリー要求を指定します。これらの値を空のままにすると、Elasticsearch Operator はデフォルト値を設定します。これらのデフォルト値はほとんどのデプロイメントでは問題なく使用できるはずです。デフォルト値は、メモリー要求の場合は **16G**、CPU 要求の場合は **1** です。

9 必要に応じて Elasticsearch プロキシーの CPU およびメモリーの制限および要求を指定します。これらの値を空のままにすると、Elasticsearch Operator はデフォルト値を設定します。これらのデフォルト値はほとんどのデプロイメントでは問題なく使用できるはずです。デフォルト値は、メモリー要求の場合は **256Mi**、CPU 要求の場合は **100m** です。

10 Kibana の設定に必要な設定。CR を使用して、冗長性を確保するために Kibana をスケーリングし、Kibana ノードの CPU およびメモリーを設定できます。詳細は、**ログビジュアライザーの設定** について参照してください。

11 Curator スケジュールの設定Curator は、OpenShift Container Platform 4.5 より前には Elasticsearch インデックス形式にあるデータを削除するために使用されましたが、今後のリリースでは削除されます。

Fluentd の設定に必要な設定。CR を使用して Fluentd の CPU およびメモリー制限を設定できます。詳細は**Fluentd の設定**を参照してください。



注記

Elasticsearch マスターノードの最大数は 3 です。**3** を超える **nodeCount** を指定する場合、OpenShift Container Platform は、マスター、クライアントおよびデータロールを使用して、3 つのマスターとしての適格性のあるノードである Elasticsearch ノードを作成します。追加の Elasticsearch ノードは、クライアントおよびデータロールを使用してデータのみのノードとして作成されます。マスターノードは、インデックスの作成および削除、シャードの割り当て、およびノードの追跡などのクラスター全体でのアクションを実行します。データノードはシャードを保持し、CRUD、検索、および集計などのデータ関連の操作を実行します。データ関連の操作は、I/O、メモリーおよび CPU 集約型の操作です。これらのリソースを監視し、現行ノードがオーバーロードする場合にデータノード追加することが重要です。

たとえば、**nodeCount=4** の場合に、以下のノードが作成されます。

```
$ oc get deployment
```

出力例

```
cluster-logging-operator       1/1     1          1          18h
elasticsearch-cd-x6kdekli-1    0/1     1          0          6m54s
elasticsearch-cdm-x6kdekli-1   1/1     1          1          18h
elasticsearch-cdm-x6kdekli-2   0/1     1          0          6m49s
elasticsearch-cdm-x6kdekli-3   0/1     1          0          6m44s
```

インデックステンプレートのプライマリーシャードの数は Elasticsearch データノードの数と等しくなります。

f. **Create** をクリックします。これにより、クラスターロギングコンポーネント、**Elasticsearch** カスタムリソースおよびコンポーネント、および Kibana インターフェイスが作成されます。

4. インストールを確認します。

a. **Workloads → Pods** ページに切り替えます。

b. **openshift-logging** プロジェクトを選択します。
以下の一覧のようなクラスターロギング、Elasticsearch、Fluentd、および Kibana のいくつかの Pod が表示されるはずです。

- cluster-logging-operator-cb795f8dc-xkckc
- elasticsearch-cdm-b3nqzchd-1-5c6797-67kfz
- elasticsearch-cdm-b3nqzchd-2-6657f4-wtprv
- elasticsearch-cdm-b3nqzchd-3-588c65-clg7g
- fluentd-2c7dg
- fluentd-9z7kk
- fluentd-br7r2
- fluentd-fn2sb
- fluentd-pb2f8
- fluentd-zqgqx
- kibana-7fb4fd4cc9-bvt4p

関連情報

- OperatorHub からの Operator のインストール

2.2. インストール後のタスク

Kibana を使用する場合、Kibana のデータを確認し、び可視化するために、Kibana インデックスパターンおよびビジュアライゼーションを手動で作成する 必要があります。

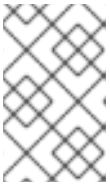
クラスターネットワークプロバイダーがネットワークの分離を実施している場合、OpenShift Logging Operator が含まれるプロジェクト間のネットワークトラフィックを許可します。

2.3. CLI を使用したクラスターロギングのインストール

OpenShift Container Platform CLI を使って Elasticsearch および Cluster Logging Operator をインストールすることができます。

前提条件

- Elasticsearch の必要な永続ストレージがあることを確認します。各 Elasticsearch ノードには独自のストレージボリュームが必要であることに注意してください。



注記

永続ストレージにローカルボリュームを使用する場合は、**LocalVolume** オブジェクトの **volumeMode: block** で記述される raw ブロックボリュームを使用しないでください。Elasticsearch は raw ブロックボリュームを使用できません。

Elasticsearch はメモリー集約型アプリケーションです。デフォルトで、OpenShift Container

Platform はメモリー要求および 16 GB の制限を持つ 3 つの Elasticsearch ノードをインストールします。OpenShift Container Platform ノードの最初の 3 つのセットには、Elasticsearch をクラスター内で実行するのに十分なメモリーがない可能性があります。Elasticsearch に関連するメモリーの問題が発生した場合、既存ノードのメモリーを増やすのではなく、Elasticsearch ノードをクラスターにさらに追加します。

手順

CLI を使用して Elasticsearch Operator および Cluster Logging Operator をインストールするには、以下を実行します。

1. Elasticsearch Operator の namespace を作成します。

   a. Elasticsearch Operator の namespace オブジェクト YAML ファイル (**eo-namespace.yaml** など) を作成します。

```
apiVersion: v1
kind: Namespace
metadata:
  name: openshift-operators-redhat (1)
  annotations:
    openshift.io/node-selector: ""
  labels:
    openshift.io/cluster-monitoring: "true" (2)
```

   (1) **openshift-operators-redhat** namespace を指定する必要があります。メトリクスとの競合が発生する可能性を防ぐには、Prometheus のクラスターモニターリングスタックを、**openshift-operators** namespace からではなく、**openshift-operators-redhat** namespace からメトリクスを収集するように設定する必要があります。**openshift-operators** namespace には信頼されていないコミュニティー Operator が含まれる可能性があり、OpenShift Container Platform メトリクスと同じ名前でメトリクスを公開する可能性があるため、これによって競合が生じる可能性があります。

   (2) クラスターモニターリングが **openshift-operators-redhat** namespace を収集できるように、このラベルを上記のように指定する必要があります。

   b. namespace を作成します。

```
$ oc create -f <file-name>.yaml
```

   以下は例になります。

```
$ oc create -f eo-namespace.yaml
```

2. Cluster Logging Operator の namespace を作成します。

   a. Cluster Logging Operator の namespace オブジェクト YAML ファイル (**clo-namespace.yaml** など) を作成します。

```
apiVersion: v1
kind: Namespace
metadata:
  name: openshift-logging
  annotations:
```

```
    openshift.io/node-selector: ""
  labels:
    openshift.io/cluster-monitoring: "true"
```

b. namespace を作成します。

```
$ oc create -f <file-name>.yaml
```

以下は例になります。

```
$ oc create -f clo-namespace.yaml
```

3. 以下のオブジェクトを作成して Elasticsearch Operator をインストールします。

a. Elasticsearch Operator の Operator グループオブジェクトの YAML ファイル (**eo-og.yaml** など) を作成します。

```
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: openshift-operators-redhat
  namespace: openshift-operators-redhat (1)
spec: {}
```

(1) **openshift-operators-redhat** namespace を指定する必要があります。

b. Operator グループオブジェクトを作成します。

```
$ oc create -f <file-name>.yaml
```

以下は例になります。

```
$ oc create -f eo-og.yaml
```

c. Subscription オブジェクト YAML ファイル (**eo-sub.yaml** など) を作成し、namespace を Elasticsearch Operator にサブスクライブします。

Subscription の例

```
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: "elasticsearch-operator"
  namespace: "openshift-operators-redhat" (1)
spec:
  channel: "4.5" (2)
  installPlanApproval: "Automatic"
  source: "redhat-operators" (3)
  sourceNamespace: "openshift-marketplace"
  name: "elasticsearch-operator"
```

(1) **openshift-operators-redhat** namespace を指定する必要があります。

2. **4.5** をチャネルとして指定します。
3. **redhat-operators** を指定します。OpenShift Container Platform クラスターが、非接続クラスターとも呼ばれるネットワークが制限された環境でインストールされている場合、Operator Lifecycle Manager (OLM) の設定時に作成される CatalogSource オブジェクトの名前を指定します。

d. Subscription オブジェクトを作成します。

```
$ oc create -f <file-name>.yaml
```

以下は例になります。

```
$ oc create -f eo-sub.yaml
```

Elasticsearch Operator は **openshift-operators-redhat** namespace にインストールされ、クラスター内の各プロジェクトにコピーされます。

e. Operator のインストールを確認します。

```
$ oc get csv --all-namespaces
```

出力例

```
NAMESPACE                                          NAME                                         DISPLAY
VERSION            REPLACES   PHASE
default                                            elasticsearch-operator.4.5.0-202007012112.p0
Elasticsearch Operator   4.5.0-202007012112.p0              Succeeded
kube-node-lease                                    elasticsearch-operator.4.5.0-202007012112.p0
Elasticsearch Operator   4.5.0-202007012112.p0              Succeeded
kube-public                                        elasticsearch-operator.4.5.0-202007012112.p0
Elasticsearch Operator   4.5.0-202007012112.p0              Succeeded
kube-system                                        elasticsearch-operator.4.5.0-202007012112.p0
Elasticsearch Operator   4.5.0-202007012112.p0              Succeeded
openshift-apiserver-operator                       elasticsearch-operator.4.5.0-
202007012112.p0    Elasticsearch Operator   4.5.0-202007012112.p0
Succeeded
openshift-apiserver                                elasticsearch-operator.4.5.0-202007012112.p0
Elasticsearch Operator   4.5.0-202007012112.p0              Succeeded
openshift-authentication-operator                  elasticsearch-operator.4.5.0-
202007012112.p0    Elasticsearch Operator   4.5.0-202007012112.p0
Succeeded
openshift-authentication                           elasticsearch-operator.4.5.0-
202007012112.p0    Elasticsearch Operator   4.5.0-202007012112.p0
Succeeded
...
```

それぞれの namespace には Elasticsearch Operator がなければなりません。バージョン番号が表示されるものと異なる場合があります。

4. 以下のオブジェクトを作成して Cluster Logging Operator をインストールします。

a. Cluster Logging Operator の OperatorGroup オブジェクトの YAML ファイル (**eo-og.yaml** など) を作成します。

```
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: cluster-logging
  namespace: openshift-logging 1
spec:
  targetNamespaces:
  - openshift-logging 2
```

1 2 **openshift-logging** namespace を指定する必要があります。

b. OperatorGroup オブジェクトを作成します。

```
$ oc create -f <file-name>.yaml
```

以下は例になります。

```
$ oc create -f clo-og.yaml
```

c. Subscription オブジェクト YAML ファイル (**clo-sub.yaml** など) を作成し、namespace を Cluster Logging Operator にサブスクライブします。

```
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: cluster-logging
  namespace: openshift-logging 1
spec:
  channel: "4.5" 2
  name: cluster-logging
  source: redhat-operators 3
  sourceNamespace: openshift-marketplace
```

1 **openshift-logging** namespace を指定する必要があります。

2 **4.5** をチャネルとして指定します。

3 **redhat-operators** を指定します。OpenShift Container Platform クラスターが、非接続クラスターとも呼ばれる制限されたネットワークにインストールされている場合、Operator Lifecycle Manager (OLM) の設定時に作成した **CatalogSource** オブジェクトの名前を指定します。

d. Subscription オブジェクトを作成します。

```
$ oc create -f <file-name>.yaml
```

以下は例になります。

```
$ oc create -f clo-sub.yaml
```

Cluster Logging Operator は **openshift-logging** namespace にインストールされます。

e. Operator のインストールを確認します。
openshift-logging namespace には Cluster Logging Operator がなければなりません。バージョン番号が表示されるものと異なる場合があります。

```
$ oc get csv -n openshift-logging
```

出力例

```
NAMESPACE                                       NAME                                         DISPLAY
VERSION            REPLACES   PHASE
...
openshift-logging                               clusterlogging.4.5.0-202007012112.p0
Cluster Logging        4.5.0-202007012112.p0            Succeeded
...
```

5. クラスターロギングのインスタンスを作成します。

a. Cluster Logging Operator のインスタンスオブジェクト YAML ファイル (**clo-instance.yaml** など) を作成します。

注記

このデフォルトのクラスターロギング設定は各種の環境をサポートすることが予想されます。クラスターロギングのクラスターに加えることのできる変更についての詳細は、クラスターロギングコンポーネントのチューニングおよび設定についてのトピックを確認してください。

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance" 1
  namespace: "openshift-logging"
spec:
  managementState: "Managed"  2
  logStore:
    type: "elasticsearch"  3
    retentionPolicy: 4
      application:
        maxAge: 1d
      infra:
        maxAge: 7d
      audit:
        maxAge: 7d
    elasticsearch:
      nodeCount: 3 5
      storage:
        storageClassName: "<storage-class-name>" 6
        size: 200G
      resources: 7
        requests:
          memory: "8Gi"
      proxy: 8
        resources:
```

```
        limits:
          memory: 256Mi
        requests:
          memory: 256Mi
    redundancyPolicy: "SingleRedundancy"
visualization:
  type: "kibana"  9
  kibana:
    replicas: 1
curation:
  type: "curator"
  curator:
    schedule: "30 3 * * *"  10
collection:
  logs:
    type: "fluentd"  11
    fluentd: {}
```

1. 名前は **instance** である必要があります。
2. クラスターロギングの管理状態。クラスターロギングのデフォルト値を変更する場合は、これを **Unmanaged** (管理外) に設定する必要がある場合があります。ただし、管理外のデプロイメントはクラスターロギングが管理対象の状態に戻されるまで更新を受信しません。デプロイメントを管理対象の状態に戻すと、加えた変更が元に戻される可能性があります。
3. Elasticsearch の設定に必要な設定。カスタムリソース (CR) を使用してシャードのレプリケーションポリシーおよび永続ストレージを設定できます。
4. Elasticsearch が各ログソースを保持する期間を指定します。整数および時間の指定 (weeks(w)、hour(h/H)、minutes(m)、および seconds(s)) を入力します。たとえば、7 日の場合は **7d** となります。**maxAge** よりも古いログは削除されます。各ログソースの保持ポリシーを指定する必要があります。そうしない場合、Elasticsearch インデックスはそのソースに対して作成されません。
5. Elasticsearch ノードの数を指定します。この一覧に続く注記を確認してください。
6. Elasticsearch ストレージの既存のストレージクラスの名前を入力します。最適なパフォーマンスを得るには、ブロックストレージを割り当てるストレージクラスを指定します。ストレージクラスを指定しない場合、OpenShift Container Platform は一時ストレージのみのクラスターロギングをデプロイします。
7. 必要に応じて CPU およびメモリー要求を指定します。これらの値を空のままにすると、Elasticsearch Operator はデフォルト値を設定します。これらのデフォルト値はほとんどのデプロイメントでは問題なく使用できるはずです。デフォルト値は、メモリー要求の場合は **16G**、CPU 要求の場合は **1** です。
8. 必要に応じて Elasticsearch プロキシーの CPU およびメモリーの制限および要求を指定します。これらの値を空のままにすると、Elasticsearch Operator はデフォルト値を設定します。これらのデフォルト値はほとんどのデプロイメントでは問題なく使用できるはずです。デフォルト値は、メモリー要求の場合は **256Mi**、CPU 要求の場合は **100m** です。
9. Kibana の設定に必要な設定。CR を使用して、冗長性を確保するために Kibana をスケーリングし、Kibana Pod の CPU およびメモリーを設定できます。詳細は、**ログビジュアライザーの設定** について参照してください。

10 Curator スケジュールの設定Curator は、OpenShift Container Platform 4.5 より前には Elasticsearch インデックス形式にあるデータを削除するために使用されましたが、

11 Fluentd の設定に必要な設定。CR を使用して Fluentd の CPU およびメモリー制限を設定できます。詳細は**Fluentd の設定**を参照してください。

注記

Elasticsearch マスターノードの最大数は 3 です。**3** を超える **nodeCount** を指定する場合、OpenShift Container Platform は、マスター、クライアントおよびデータロールを使用して、3 つのマスターとしての適格性のあるノードである Elasticsearch ノードを作成します。追加の Elasticsearch ノードは、クライアントおよびデータロールを使用してデータのみのノードとして作成されます。マスターノードは、インデックスの作成および削除、シャードの割り当て、およびノードの追跡などのクラスター全体でのアクションを実行します。データノードはシャードを保持し、CRUD、検索、および集計などのデータ関連の操作を実行します。データ関連の操作は、I/O、メモリーおよび CPU 集約型の操作です。これらのリソースを監視し、現行ノードがオーバーロードする場合にデータノード追加することが重要です。

たとえば、**nodeCount=4** の場合に、以下のノードが作成されます。

```
$ oc get deployment
```

出力例

```
cluster-logging-operator       1/1     1          1          18h
elasticsearch-cd-x6kdekli-1    1/1     1          0          6m54s
elasticsearch-cdm-x6kdekli-1   1/1     1          1          18h
elasticsearch-cdm-x6kdekli-2   1/1     1          0          6m49s
elasticsearch-cdm-x6kdekli-3   1/1     1          0          6m44s
```

インデックステンプレートのプライマリーシャードの数は Elasticsearch データノードの数と等しくなります。

b. インスタンスを作成します。

```
$ oc create -f <file-name>.yaml
```

以下は例になります。

```
$ oc create -f clo-instance.yaml
```

これにより、クラスターロギングコンポーネント、**Elasticsearch** カスタムリソースおよびコンポーネント、および Kibana インターフェイスが作成されます。

6. **openshift-logging** プロジェクトに Pod を一覧表示して、インストールを検証します。
以下の一覧のようなクラスターロギング、Elasticsearch、Fluentd、および Kibana のいくつかの Pod が表示されるはずです。

```
$ oc get pods -n openshift-logging
```

出力例

```
NAME                                            READY   STATUS    RESTARTS   AGE
cluster-logging-operator-66f77ffccb-ppzbg       1/1     Running   0          7m
elasticsearch-cdm-ftuhduuw-1-ffc4b9566-q6bhp    2/2     Running   0          2m40s
elasticsearch-cdm-ftuhduuw-2-7b4994dbfc-rd2gc   2/2     Running   0          2m36s
elasticsearch-cdm-ftuhduuw-3-84b5ff7ff8-gqnm2   2/2     Running   0          2m4s
fluentd-587vb                                   1/1     Running   0          2m26s
fluentd-7mpb9                                   1/1     Running   0          2m30s
fluentd-flm6j                                   1/1     Running   0          2m33s
fluentd-gn4rn                                   1/1     Running   0          2m26s
fluentd-nlgb6                                   1/1     Running   0          2m30s
fluentd-snpkt                                   1/1     Running   0          2m28s
kibana-d6d5668c5-rppqm                          2/2     Running   0          2m39s
```

2.4. インストール後のタスク

Kibana を使用する場合、Kibana のデータを確認し、び可視化するために、Kibana インデックスパターンおよびビジュアライゼーションを手動で作成する 必要があります。

クラスターネットワークプロバイダーがネットワークの分離を実施している場合、OpenShift Logging Operator が含まれるプロジェクト間のネットワークトラフィックを許可します。

2.4.1. Kibana インデックスパターンの定義

インデックスパターンは、可視化する必要のある Elasticsearch インデックスを定義します。Kibana でデータを確認し、可視化するには、インデックスパターンを作成する必要があります。

前提条件

- Kibana で **infra** および **audit** インデックスを表示するには、ユーザーには **cluster-admin** ロール、 **cluster-reader** ロール、または両方のロールが必要です。デフォルトの **kubeadmin** ユーザーには、これらのインデックスを表示するための適切なパーミッションがあります。**default**、**kube-** および **openshift-** プロジェクトで Pod およびログを表示できる場合、これらのインデックスにアクセスできるはずです。以下のコマンドを使用して、現在のユーザーが適切なパーミッションを持っているかどうかを確認することができます。

```
$ oc auth can-i get pods/log -n <project>
```

出力例

```
yes
```

注記

監査ログは、デフォルトでは内部 OpenShift Container Platform Elasticsearch インスタンスに保存されません。Kibana で監査ログを表示するには、ログ転送 API を使用して監査ログの **default** 出力を使用するパイプラインを設定する必要があります。

- Elasticsearch ドキュメントは、インデックスパターンを作成する前にインデックス化する必要があります。これは自動的に実行されますが、新規または更新されたクラスターでは数分の時間がかかる可能性があります。

手順

Kibana でインデックスパターンを定義し、ビジュアライゼーションを作成するには、以下を実行します。

1. OpenShift Container Platform コンソールで、Application Launcher  をクリックし、**Logging** を選択します。

2. **Management → Index Patterns → Create index pattern** をクリックして Kibana インデックスパターンを作成します。

   - 各ユーザーは、プロジェクトのログを確認するために、Kibana に初めてログインする際にインデックスパターンを手動で作成する必要があります。ユーザーは **app** という名前のインデックスパターンを作成し、**@timestamp** 時間フィールドを使用してコンテナーログを表示する必要があります。

   - 管理ユーザーはそれぞれ、最初に Kibana にログインする際に、**@timestamp** 時間フィールドを使用して **app**、 **infra** および **audit** インデックスについてインデックスパターンを作成する必要があります。

3. 新規インデックスパターンから Kibana のビジュアライゼーション (Visualization) を作成します。

2.4.2. ネットワークの分離が有効にされている場合のプロジェクト間のトラフィックの許可

クラスターネットワークプロバイダーはネットワークの分離を有効にする可能性があります。その場合、OpenShift Logging によってデプロイされる Operator が含まれるプロジェクト間のネットワークトラフィックを許可する必要があります。

ネットワークの分離は、異なるプロジェクトにある Pod およびサービス間のネットワークトラフィックをブロックします。OpenShift Logging は、**OpenShift Elasticsearch Operator** を **openshift-operators-redhat** プロジェクトにインストールし、**Red Hat OpenShift Logging Operator** を **openshift-logging** プロジェクトにインストールします。したがって、これら 2 つのプロジェクト間のトラフィックを許可する必要があります。

OpenShift Container Platform は、2 つのサポート対象のオプションをデフォルトの Container Network Interface (CNI) ネットワークプロバイダー、OpenShift SDN および OVN-Kubernetes 用に提供します。これら 2 つのプロバイダーはさまざまなネットワーク分離ポリシーを実装します。

OpenShift SDN には 3 つのモードがあります。

network policy (ネットワークポリシー)

これはデフォルトモードになります。ポリシーが定義されていない場合は、すべてのトラフィックを許可します。ただし、ユーザーがポリシーを定義する場合、通常はすべてのトラフィックを拒否し、例外を追加して開始します。このプロセスでは、異なるプロジェクトで実行されているアプリケーションが破損する可能性があります。そのため、ポリシーを明示的に設定し、1 つのロギング関連のプロジェクトから他のプロジェクトへの egress のトラフィックを許可します。

multitenant (マルチテナント)

このモードは、ネットワークの分離を実行します。2 つのロギング関連のプロジェクトを結合して、それらのプロジェクト間のトラフィックを許可します。

subnet (サブネット)

このモードでは、すべてのトラフィックを許可します。ネットワーク分離は実行しません。アクションは不要です。

OVN-Kubernetes は常に **ネットワークポリシー** を使用します。そのため、OpenShift SDN の場合と同様に、ポリシーを明示的に設定し、1 つのロギング関連のプロジェクトから他のプロジェクトへの egress のトラフィックを許可する必要があります。

手順

- **multitenant** モードで OpenShift SDN を使用している場合は、2 つのプロジェクトに参加します。以下に例を示します。

```
$ oc adm pod-network join-projects --to=openshift-operators-redhat openshift-logging
```

- または、**network policy** の OpenShift SDN および OVN-Kubernetes の場合は、以下の操作を実行します。

a. **openshift-operators-redhat** namespace にラベルを設定します。以下に例を示します。

```
$ oc label namespace openshift-operators-redhat project=openshift-operators-redhat
```

b. **openshift-logging** namespace で、 **openshift-operators-redhat** プロジェクトから **openshift-logging** プロジェクトへの ingress を許可するネットワークポリシーオブジェクトを作成します。以下に例を示します。

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: allow-openshift-operators-redhat
spec:
  ingress:
    - from:
      - namespaceSelector:
          matchLabels:
            project: openshift-operators-redhat
```

関連情報

- ネットワークポリシーについて
- OpenShift SDN デフォルト CNI ネットワークプロバイダーについて
- OVN-Kubernetes デフォルト Container Network Interface (CNI) ネットワークプロバイダーについて

第3章 クラスターロギングデプロイメントの設定

3.1. クラスターロギングカスタムリソースについて

OpenShift Container Platform クラスターロギングを設定するには、**ClusterLogging** カスタムリソース (CR) をカスタマイズします。

3.1.1. ClusterLogging カスタムリソースについて

クラスターロギング環境を変更するには、**ClusterLogging** カスタムリソース (CR) を作成し、変更します。

CR の作成または変更方法については、このドキュメントで適宜説明されます。

以下は、クラスターロギングの通常のカスタムリソースの例です。

ClusterLogging カスタムリソース (CRD) のサンプル

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance" 1
  namespace: "openshift-logging" 2
spec:
  managementState: "Managed" 3
  logStore:
    type: "elasticsearch" 4
    retentionPolicy:
      application:
        maxAge: 1d
      infra:
        maxAge: 7d
      audit:
        maxAge: 7d
    elasticsearch:
      nodeCount: 3
      resources:
        limits:
          memory: 16Gi
        requests:
          cpu: 500m
          memory: 16Gi
      storage:
        storageClassName: "gp2"
        size: "200G"
      redundancyPolicy: "SingleRedundancy"
  visualization: 5
    type: "kibana"
    kibana:
      resources:
        limits:
          memory: 736Mi
        requests:
          cpu: 100m
```

```
        memory: 736Mi
    replicas: 1
  curation: 6
    type: "curator"
    curator:
      resources:
        limits:
          memory: 256Mi
        requests:
          cpu: 100m
          memory: 256Mi
      schedule: "30 3 * * *"
  collection: 7
    logs:
      type: "fluentd"
      fluentd:
        resources:
          limits:
            memory: 736Mi
          requests:
            cpu: 100m
            memory: 736Mi
```

1. CR の名前は **instance** である必要があります。
2. CR は **openshift-logging** namespace にインストールされる必要があります。
3. Cluster Logging Operator の管理状態。**Unmanaged** に設定すると、Operator はサポート対象外となり、更新を取得しません。
4. 保持ポリシー、ノード数、リソース要求および制限およびストレージクラスなどのログストアの設定。
5. リソース要求および制限、Pod レプリカ数などのビジュアライザーの設定。
6. リソースの要求および制限、および収集スケジュールを含む、収集についての設定。
7. リソース要求および制限を含むログコレクターの設定。

3.2. ロギングコレクターの設定

OpenShift Container Platform は Fluentd を使用して、クラスターから操作およびアプリケーションログを収集し、Kubernetes Pod およびプロジェクトメタデータでデータを拡充します。

ログコレクターの CPU およびメモリー制限を設定し、ログコレクター Pod を特定のノードに移動 できます。ログコレクターに対するサポートされるすべての変更は、**ClusterLogging** カスタムリソース (CR) の **spec.collection.log.fluentd** スタンザを使用して実行できます。

3.2.1. サポートされる設定

クラスターロギングの設定のサポートされる方法として、本書で説明されているオプションを使用してこれを設定することができます。サポートされていない他の設定は使用しないでください。設定のパラダイムが OpenShift Container Platform リリース間で変更される可能性があり、このような変更は、設

定のすべての可能性が制御されている場合のみ適切に対応できます。本書で説明されている設定以外の設定を使用する場合、Elasticsearch Operator および Cluster Logging Operator が差分を調整するため、変更内容は失われます。Operator はデフォルトで定義された状態にすべて戻します。

注記

OpenShift Container Platform ドキュメントで説明されていない設定を実行する **必要がある** 場合、Cluster Logging Operator または Elasticsearch Operator を **Unmanaged** (管理外) に設定する **必要があります**。管理外のクラスターロギング環境は **サポート対象外** であり、クラスターロギングを **Managed** に戻すまで変更を受信しません。

3.2.2. ロギングコレクター Pod の表示

oc get pods --all-namespaces -o wide コマンドを使用して、Fluentd がデプロイされるノードを表示できます。

手順

openshift-logging プロジェクトで以下のコマンドを実行します。

```
$ oc get pods --selector component=fluentd -o wide -n openshift-logging
```

出力例

```
NAME          READY  STATUS    RESTARTS   AGE     IP           NODE              NOMINATED
NODE   READINESS GATES
fluentd-8d69v  1/1    Running   0          134m    10.130.2.30   master1.example.com   <none>
<none>
fluentd-bd225  1/1    Running   0          134m    10.131.1.11   master2.example.com   <none>
<none>
fluentd-cvrzs  1/1    Running   0          134m    10.130.0.21   master3.example.com   <none>
<none>
fluentd-gpqg2  1/1    Running   0          134m    10.128.2.27   worker1.example.com   <none>
<none>
fluentd-l9j7j  1/1    Running   0          134m    10.129.2.31   worker2.example.com   <none>
<none>
```

3.2.3. ログコレクター CPU およびメモリー制限の設定

ログコレクターは、CPU とメモリー制限の両方への調整を許可します。

手順

1. **openshift-logging** プロジェクトで **ClusterLogging** カスタムリソース (CR) を編集します。

```
$ oc edit ClusterLogging instance
```

```
$ oc edit ClusterLogging instance

apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"
```

```
....

spec:
  collection:
    logs:
      fluentd:
        resources:
          limits: 1
            memory: 736Mi
          requests:
            cpu: 100m
            memory: 736Mi
```

1 必要に応じて CPU、メモリー制限および要求を指定します。表示される値はデフォルト値です。

3.2.4. ロギングコレクターのアラートについて

以下のアラートはロギングコレクターによって生成されます。これらのアラートは、OpenShift Container Platform Web コンソールの Alerting UI の **Alerts** ページで表示できます。

表3.1 Fluentd Prometheus アラート

アラート	メッセージ	説明	重大度
FluentdErrorsHigh	**In the last minute, <value> errors reported by fluentd <instance>.**	Fluentd は指定した数 (デフォルトでは 10) よりも多くの問題を報告しています。	Critical
FluentdNodeDown	**Prometheus could not scrape fluentd <instance> for more than 10m.**	Fluentd は Prometheus が特定の Fluentd インスタンスを収集できなかったことを報告します。	Critical
FluentdQueueLengthBurst	**In the last minute, fluentd <instance> buffer queue length increased more than 32.Current value is <value>.**	Fluentd は値が大きすぎることを報告しています。	Warning
FluentdQueueLengthIncreasing	**In the last 12h, fluentd <instance> buffer queue length constantly increased more than 1.Current value is <value>.**	Fluentd はキューの使用についての問題を報告しています。	Critical

3.2.5. デフォルトの Elasticsearch ログストアを使用しない場合の未使用のコンポーネントの削除

管理者がログをサードパーティーのログストアに転送し、デフォルトの Elasticsearch ログストアを使用しない場合には、ロギングクラスターからいくつかの未使用のコンポーネントを削除できます。

つまり、デフォルトの Elasticsearch ログストアを使用しない場合、内部 Elasticsearch **logStore**、Kibana **visualization**、およびログ **curation** コンポーネントを **ClusterLogging** カスタムリソース (CR) から削除することができます。これらのコンポーネントの削除はオプションですが、これによりリソースを節約できます。

前提条件

- ログフォワーダーがログデータをデフォルトの内部 Elasticsearch クラスターに送信しないことを確認します。ログ転送の設定に使用した **ClusterLogForwarder** CR YAML ファイルを検査します。これには **default** を指定する **outputRefs** 要素が **ない** ことを確認します。以下に例を示します。

```
outputRefs:
- default
```

警告

ClusterLogForwarder CR がログデータを内部 Elasticsearch クラスターに転送し、**ClusterLogging** CR から **logStore** コンポーネントを削除するとします。この場合、内部 Elasticsearch クラスターはログデータを保存するために表示されません。これがないと、データが失われる可能性があります。

手順

1. **openshift-logging** プロジェクトで **ClusterLogging** カスタムリソース (CR) を編集します。

```
$ oc edit ClusterLogging instance
```

2. これらが存在する場合、**logStore**、**visualization**、 **curation** スタンザを **ClusterLogging** CR から削除します。

3. **ClusterLogging** CR の **collection** スタンザを保持します。結果は以下の例のようになります。

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"
  namespace: "openshift-logging"
spec:
  managementState: "Managed"
  collection:
    logs:
      type: "fluentd"
      fluentd: {}
```

4. Flunentd Pod が再デプロイされていることを確認します。

```
$ oc get pods -n openshift-logging
```

追加リソース

- ログのサードパーティーシステムへの転送

3.3. ログストアの設定

OpenShift Container Platform は Elasticsearch 6 (ES) を使用してログデータを保存し、整理します。

ログストアに加えることのできる変更には、以下が含まれます。

- Elasticsearch クラスターのストレージ。
- シャードをクラスター内の複数のデータノードにレプリケートする方法 (完全なレプリケーションからレプリケーションなしまで)。
- Elasticsearch データへの外部アクセス

Elasticsearch はメモリー集約型アプリケーションです。それぞれの Elasticsearch ノードには、**ClusterLogging** カスタムリソースで指定しない限り、メモリー要求および制限の両方に 16G のメモリーが必要です。初期設定の OpenShift Container Platform ノードのセットは、Elasticsearch クラスターをサポートするのに十分な大きさではない場合があります。その場合、推奨されるサイズ以上のメモリーを使用して実行できるようにノードを OpenShift Container Platform クラスターに追加する必要があります。

各 Elasticsearch ノードはこれより低い値のメモリー設定でも動作しますが、これは実稼働環境には推奨されません。

3.3.1. 監査ログのログストアへの転送

内部 OpenShift Container Platform Elasticsearch ログストアは監査ログのセキュアなストレージを提供しないため、デフォルトで監査ログは内部 Elasticsearch インスタンスに保存されません。

監査ログを内部ログストアに送信する必要がある場合 (Kibana で監査ログを表示するなど)、ログ転送 API を使用する必要があります。ログ転送 API は現時点ではテクノロジープレビュー機能です。

重要

内部 OpenShift Container Platform Elasticsearch ログストアは、監査ログのセキュアなストレージを提供しません。監査ログを転送するシステムが組織および政府の規制に準拠しており、適切にセキュリティーが保護されていることを確認することが推奨されています。OpenShift Container Platform クラスターロギングはこれらの規制に準拠しません。

手順

ログ転送 API を使用して監査ログを内部 Elasticsearch インスタンスに転送するには、以下を実行します。

1. ログ転送 API が有効にされていない場合:
   a. **openshift-logging** プロジェクトで **ClusterLogging** カスタムリソース (CR) を編集します。

```
$ oc edit ClusterLogging instance
```

b. **clusterlogging.openshift.io/logforwardingtechpreview** アノテーションを追加し、**enabled** に設定します。

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  annotations:
    clusterlogging.openshift.io/logforwardingtechpreview: enabled (1)
  name: "instance"
  namespace: "openshift-logging"
spec:

...

  collection: (2)
    logs:
      type: "fluentd"
      fluentd: {}
```

(1) ログ転送 API を有効および無効にします。ログ転送を使用するには、**enabled** に設定します。

(2) Fluentd を使用できるように、**spec.collection** ブロックを **ClusterLogging** CR で定義する必要があります。

2. **LogForwarding** CR YAML ファイルを作成するか、または既存の CR を編集します。

- すべてのログタイプを内部 Elasticsearch インスタンスに送信するために CR を作成します。変更せずに以下の例を使用できます。

```
apiVersion: logging.openshift.io/v1alpha1
kind: LogForwarding
metadata:
  name: instance
  namespace: openshift-logging
spec:
  disableDefaultForwarding: true
  outputs:
    - name: clo-es
      type: elasticsearch
      endpoint: 'elasticsearch.openshift-logging.svc:9200' (1)
      secret:
        name: fluentd
  pipelines:
    - name: audit-pipeline (2)
      inputSource: logs.audit
      outputRefs:
        - clo-es
    - name: app-pipeline (3)
      inputSource: logs.app
      outputRefs:
        - clo-es
```

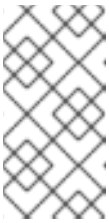
```
 - name: infra-pipeline 4
   inputSource: logs.infra
   outputRefs:
     - clo-es
```

1 **endpoint** パラメーターは内部 Elasticsearch インスタンスを参照します。

2 このパラメーターは、監査ログを指定されたエンドポイントに送信します。

3 このパラメーターは、アプリケーションログを指定されたエンドポイントに送信します。

4 このパラメーターは、インフラストラクチャーログを指定されたエンドポイントに送信します。



注記

アプリケーション、インフラストラクチャーおよび監査の 3 つの種類のログすべてのパイプラインおよび出力を設定する必要があります。ログの種類に対応するパイプラインおよび出力を指定しない場合、それらのログは保存されず、失われます。

- 既存の **LogForwarding** CR がある場合、内部 Elasticsearch インスタンスの出力およびパイプラインを監査ログの出力に追加します。以下は例になります。

```
apiVersion: "logging.openshift.io/v1alpha1"
kind: "LogForwarding"
metadata:
  name: instance
  namespace: openshift-logging
spec:
  disableDefaultForwarding: true
  outputs:
   - name: elasticsearch 1
     type: "elasticsearch"
     endpoint: elasticsearch.openshift-logging.svc:9200
     secret:
       name: fluentd
   - name: elasticsearch-insecure
     type: "elasticsearch"
     endpoint: elasticsearch-insecure.messaging.svc.cluster.local
     insecure: true
   - name: secureforward-offcluster
     type: "forward"
     endpoint: https://secureforward.offcluster.com:24224
     secret:
       name: secureforward
  pipelines:
   - name: container-logs
     inputSource: logs.app
     outputRefs:
     - secureforward-offcluster
   - name: infra-logs
     inputSource: logs.infra
```

```
    outputRefs:
    - elasticsearch-insecure
  - name: audit-logs (2)
    inputSource: logs.audit
    outputRefs:
    - elasticsearch
```

(1) 内部 Elasticsearch インスタンスの出力。

(2) 監査ログを内部 Elasticsearch インスタンスに送信するためのパイプライン。

追加リソース

ログ転送 API の詳細は、Forwarding logs using the Log Forwarding API を参照してください。

3.3.2. ログ保持時間の設定

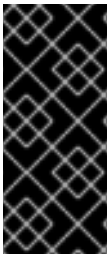
デフォルトの Elasticsearch ログストアが、インフラストラクチャーログ、アプリケーションログ、監査ログなどの 3 つのログソースごとに個別の **保持ポリシー** を使用してインデックスを保持する期間を指定できます。クラスターロギングのカスタムリソース (CR) で **maxAge** パラメーターを使用して設定する保持ポリシーは、Elasticsearch のロールオーバースケジュールに関連して考慮され、Elasticseach がロールオーバーインデックスを削除するタイミングを決定します。

Elasticsearch はインデックスをロールオーバーし、インデックスが以下の条件のいずれかに一致する場合に現在のインデックスを移動し、新規インデックスを作成します。

- インデックスは **Elasticsearch** CR の **rollover.maxAge** の値よりも古い値になります。
- インデックスサイズは、40 GB x プライマリーシャードの数よりも大きくなります。
- インデックスの doc 数は、40960 KB × プライマリーシャードの数よりも大きくなります。

Elasticsearch は、設定する保持ポリシーに基づいてロールオーバーインデックスを削除します。

ログソースの保持ポリシーを作成しないと、ログはデフォルトで 7 日後に削除されます。



重要

3 つのすべてのログソースに保持ポリシーを指定しない場合、保持ポリシーが指定されたソースのログのみが保存されます。たとえば、インフラストラクチャーおよびアプリのログの保持ポリシーを設定し、監査ログの保持ポリシーを設定しない場合、監査ログは保持されず、Elasticsearch または Kibana に **audit-** インデックスは存在しなくなります。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

ログの保持時間を設定するには、以下を実行します。

1. **ClusterLogging** CR を編集して、**retentionPolicy** パラメーターを追加するか、または変更します。

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
...
spec:
  managementState: "Managed"
  logStore:
    type: "elasticsearch"
    retentionPolicy: (1)
      application:
        maxAge: 1d
      infra:
        maxAge: 7d
      audit:
        maxAge: 7d
    elasticsearch:
      nodeCount: 3
...
```

(1) Elasticsearch が各ログソースを保持する時間を指定します。整数および時間の指定 (weeks(w)、hour(h/H)、minutes(m)、および seconds(s)) を入力します。たとえば、1 日の場合は **1d** になります。**maxAge** よりも古いログは削除されます。デフォルトで、ログは 7 日間保持されます。

2. **Elasticsearch** カスタムリソース (CR) で設定を確認できます。
たとえば、Cluster Logging Operator は以下の **Elasticsearch** CR を更新し、8 時間ごとにインフラストラクチャーログのアクティブなインデックスをロールオーバーし、ロールオーバーされたインデックスはロールオーバーの 7 日後に削除される設定を含む保持ポリシーを設定するとします。OpenShift Container Platform は 15 分ごとにチェックし、インデックスをロールオーバーする必要があるかどうかを判別します。

```
apiVersion: "logging.openshift.io/v1"
kind: "Elasticsearch"
metadata:
  name: "elasticsearch"
spec:
...
  indexManagement:
    policies: (1)
      - name: infra-policy
        phases:
          delete:
            minAge: 7d (2)
          hot:
            actions:
              rollover:
                maxAge: 8h (3)
        pollInterval: 15m (4)
...
```

(1) 各ログソースについて、保持ポリシーは、そのソースのログを削除/ロールオーバーするタイミングを示します。

(2) OpenShift Container Platform がロールオーバーされたインデックスを削除する場合。この設定は、**ClusterLogging** CR に設定する **maxAge** になります。

3 インデックスをロールオーバーする際に考慮する OpenShift Container Platform のインデックス期間。この値は、**ClusterLogging** CR に設定する **maxAge** に基づいて決定され

4 OpenShift Container Platform がインデックスをロールオーバーする必要があるかどうかをチェックする場合。この設定はデフォルトであるため、変更できません。

注記

Elasticsearch CR の変更はサポートされていません。保持ポリシーに対するすべての変更は **ClusterLogging** CR で行う必要があります。

Elasticsearch Operator は cron ジョブをデプロイし、**pollInterval** を使用してスケジュールされる定義されたポリシーを使用して各マッピングのインデックスをロールオーバーします。

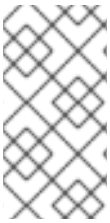
```
$ oc get cronjobs
```

出力例

```
NAME                     SCHEDULE      SUSPEND   ACTIVE   LAST SCHEDULE   AGE
elasticsearch-delete-app      */15 * * * *   False     0        <none>          27s
elasticsearch-delete-audit    */15 * * * *   False     0        <none>          27s
elasticsearch-delete-infra    */15 * * * *   False     0        <none>          27s
elasticsearch-rollover-app    */15 * * * *   False     0        <none>          27s
elasticsearch-rollover-audit  */15 * * * *   False     0        <none>          27s
elasticsearch-rollover-infra  */15 * * * *   False     0        <none>          27s
```

3.3.3. ログストアの CPU およびメモリー要求の設定

それぞれのコンポーネント仕様は、CPU とメモリー要求の両方への調整を許可します。Elasticsearch Operator は環境に適した値を設定するため、これらの値を手動で調整する必要はありません。



注記

大規模なクラスターでは、Elasticsearch プロキシーコンテナーのデフォルトのメモリー制限が不十分である場合があり、これにより、プロキシーコンテナーが OOM による強制終了 (OOMKilled) が生じます。この問題が発生した場合には、Elasticsearch プロキシーのメモリー要求および制限を引き上げます。

各 Elasticsearch ノードはこれより低い値のメモリー設定でも動作しますが、これは実稼働環境でのデプロイメントには推奨 **されていません**。実稼働環境での使用の場合には、デフォルトの 16Gi よりも小さい値を各 Pod に割り当てることはできません。Pod ごとに割り当て可能な最大値は 64Gi であり、この範囲の中で、できるだけ多くのメモリーを割り当てることを推奨します。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

1. **openshift-logging** プロジェクトで **ClusterLogging** カスタムリソース (CR) を編集します。

```
$ oc edit ClusterLogging instance
```

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"
....
spec:
    logStore:
      type: "elasticsearch"
      elasticsearch:
        resources: 1
          limits:
            memory: 16Gi
          requests:
            cpu: "1"
            memory: "64Gi"
        proxy: 2
          resources:
            limits:
              memory: 100Mi
            requests:
              memory: 100Mi
```

1 必要に応じて CPU およびメモリー要求を指定します。これらの値を空のままにすると、Elasticsearch Operator はデフォルト値を設定します。これらのデフォルト値はほとんどのデプロイメントでは問題なく使用できるはずです。デフォルト値は、メモリー要求の場合は **16Gi** であり、CPU 要求の場合は **1** です。

2 必要に応じて Elasticsearch プロキシーの CPU およびメモリーの制限および要求を指定します。これらの値を空のままにすると、Elasticsearch Operator はデフォルト値を設定します。これらのデフォルト値はほとんどのデプロイメントでは問題なく使用できるはずです。デフォルト値は、メモリー要求の場合は **256Mi**、CPU 要求の場合は **100m** です。

Elasticsearch メモリーの容量を調整する場合、要求値と制限値の両方を変更する必要があります。

以下は例になります。

```
resources:
  limits:
    cpu: "8"
    memory: "32Gi"
  requests:
    cpu: "8"
    memory: "32Gi"
```

Kubernetes は一般的にはノードの設定に従い、Elasticsearch が指定された制限を使用することを許可しません。**requests** と **limites** に同じ値を設定することにより、Elasticsearch は必要な CPU およびメモリーを確実に使用できるようにします (利用可能な CPU およびメモリーがノードにあることを前提とします)。

3.3.4. ログストアのレプリケーションポリシーの設定

Elasticsearch シャードをクラスター内の複数のデータノードにレプリケートする方法を定義できます。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

1. **openshift-logging** プロジェクトで **ClusterLogging** カスタムリソース (CR) を編集します。

```
$ oc edit clusterlogging instance
```

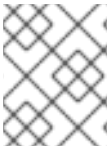
```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"

....

spec:
  logStore:
    type: "elasticsearch"
    elasticsearch:
      redundancyPolicy: "SingleRedundancy" (1)
```

(1) シャードの冗長性ポリシーを指定します。変更の保存時に変更が適用されます。

- **FullRedundancy**:Elasticsearch は、各インデックスのプライマリーシャードをすべてのデータノードに完全にレプリケートします。これは最高レベルの安全性を提供しますが、最大量のディスクが必要となり、パフォーマンスは最低レベルになります。
- **MultipleRedundancy**:Elasticsearch は、各インデックスのプライマリーシャードをデータノードの半分に完全にレプリケートします。これは、安全性とパフォーマンス間の適切なトレードオフを提供します。
- **SingleRedundancy**:Elasticsearch は、各インデックスのプライマリーシャードのコピーを 1 つ作成します。2 つ以上のデータノードが存在する限り、ログは常に利用可能かつ回復可能です。5 以上のノードを使用する場合には、MultipleRedundancy よりもパフォーマンスが良くなります。このポリシーは、単一 Elasticsearch ノードのデプロイメントには適用できません。
- **ZeroRedundancy**:Elasticsearch は、プライマリーシャードのコピーを作成しません。ノードが停止または失敗した場合、ログは利用不可となるか、失われる可能性があります。安全性よりもパフォーマンスを重視する場合や、独自のディスク/PVC バックアップ/復元ストラテジーを実装している場合は、このモードを使用できます。



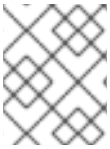
注記

インデックステンプレートのプライマリーシャードの数は Elasticsearch データノードの数と等しくなります。

3.3.5. Elasticsearch Pod のスケールダウン

クラスター内の Elasticsearch Pod 数を減らすと、データ損失や Elasticsearch のパフォーマンスが低下する可能性があります。

スケールダウンする場合、一度に 1 つの Pod 分スケールダウンし、クラスターがシャードおよびレプリカのリバランスを実行できるようにする必要があります。Elasticsearch のヘルスステータスが **green** に戻された後に、別の Pod でスケールダウンできます。



注記

Elasticsearch クラスターが **ZeroRedundancy** に設定される場合、Elasticsearch Pod をスケールダウンしないでください。

3.3.6. ログストアの永続ストレージの設定

Elasticsearch には永続ストレージが必要です。ストレージが高速になると、Elasticsearch のパフォーマンスも高速になります。

警告

NFS ストレージをボリュームまたは永続ボリュームを使用 (または Gluster などの NAS を使用する) ことは Elasticsearch ストレージではサポートされません。Lucene は NFS が指定しないファイルシステムの動作に依存するためです。データの破損およびその他の問題が発生する可能性があります。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

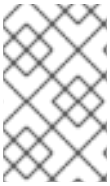
1. **ClusterLogging** CR を編集してクラスターの各データノードが永続ボリューム要求 (PVC) にバインドされるように指定します。

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"

....

 spec:
    logStore:
      type: "elasticsearch"
      elasticsearch:
        nodeCount: 3
        storage:
          storageClassName: "gp2"
          size: "200G"
```

この例では、クラスターの各データノードが、200G の AWS General Purpose SSD (gp2) ストレージを要求する永続ボリューム要求 (PVC) にバインドされるように指定します。



注記

永続ストレージにローカルボリュームを使用する場合は、**LocalVolume** オブジェクトの **volumeMode: block** で記述される raw ブロックボリュームを使用しないでください。Elasticsearch は raw ブロックボリュームを使用できません。

3.3.7. emptyDir ストレージのログストアの設定

ログストアで emptyDir を使用することができます。これは、Pod のデータすべてが再起動時に失われる一時デプロイメントを作成します。

注記

emptyDir を使用する場合、ログストアが再起動するか、または再デプロイされる場合にデータが失われます。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

1. **ClusterLogging** CR を編集して emptyDir を指定します。

```
spec:
  logStore:
    type: "elasticsearch"
    elasticsearch:
      nodeCount: 3
      storage: {}
```

3.3.8. Elasticsearch クラスターのローリング再起動の実行

elasticsearch configmap または **elasticsearch-*** デプロイメント設定のいずれかを変更する際にローリング再起動を実行します。

さらにローリング再起動は、Elasticsearch Pod が実行されるノードで再起動が必要な場合に推奨されます。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。
- OpenShift Container Platform の es_util ツールをインストールします。

手順

クラスターのローリング再起動を実行するには、以下を実行します。

1. **openshift-logging** プロジェクトに切り替えます。

```
$ oc project openshift-logging
```

2. Elasticsearch Pod の名前を取得します。

```
$ oc get pods | grep elasticsearch-
```

3. OpenShift Container Platform **es_util** ツールを使用してシャードの同期フラッシュを実行して、シャットダウンの前にディスクへの書き込みを待機している保留中の操作がないようにします。

```
$ oc exec <any_es_pod_in_the_cluster> -c elasticsearch -- es_util --query="_flush/synced" -XPOST
```

以下に例を示します。

```
$ oc exec -c elasticsearch-cdm-5ceex6ts-1-dcd6c4c7c-jpw6  -c elasticsearch -- es_util --query="_flush/synced" -XPOST
```

出力例

```
{"_shards":{"total":4,"successful":4,"failed":0},".security":{"total":2,"successful":2,"failed":0},".kibana_1":{"total":2,"successful":2,"failed":0}}
```

4. OpenShift Container Platform es_util ツールを使用して、ノードを意図的に停止する際のシャードのバランシングを防ぎます。

```
$ oc exec <any_es_pod_in_the_cluster> -c elasticsearch -- es_util --query="_cluster/settings" -XPUT -d '{ "persistent": { "cluster.routing.allocation.enable" : "primaries" } }'
```

以下に例を示します。

```
$ oc exec elasticsearch-cdm-5ceex6ts-1-dcd6c4c7c-jpw6 -c elasticsearch -- es_util --query="_cluster/settings" -XPUT -d '{ "persistent": { "cluster.routing.allocation.enable" : "primaries" } }'
```

出力例

```
{"acknowledged":true,"persistent":{"cluster":{"routing":{"allocation":{"enable":"primaries"}}}},"transient":
```

5. コマンドが完了したら、ES クラスターのそれぞれのデプロイメントについて、以下を実行します。

   a. デフォルトで、OpenShift Container Platform Elasticsearch クラスターはノードのロールアウトをブロックします。以下のコマンドを使用してロールアウトを許可し、Pod が変更を取得できるようにします。

   ```
   $ oc rollout resume deployment/<deployment-name>
   ```

   以下に例を示します。

```
$ oc rollout resume deployment/elasticsearch-cdm-0-1
```

出力例

```
deployment.extensions/elasticsearch-cdm-0-1 resumed
```

新規 Pod がデプロイされます。Pod に準備状態のコンテナーがある場合、次のデプロイメントに進むことができます。

```
$ oc get pods | grep elasticsearch-
```

出力例

```
NAME                                  READY   STATUS    RESTARTS   AGE
elasticsearch-cdm-5ceex6ts-1-dcd6c4c7c-jpw6k   2/2     Running   0          22h
elasticsearch-cdm-5ceex6ts-2-f799564cb-l9mj7   2/2     Running   0          22h
elasticsearch-cdm-5ceex6ts-3-585968dc68-k7kjr   2/2     Running   0          22h
```

b. デプロイメントが完了したら、ロールアウトを許可しないように Pod をリセットします。

```
$ oc rollout pause deployment/<deployment-name>
```

以下に例を示します。

```
$ oc rollout pause deployment/elasticsearch-cdm-0-1
```

出力例

```
deployment.extensions/elasticsearch-cdm-0-1 paused
```

c. Elasticsearch クラスターが **green** または **yellow** 状態にあることを確認します。

```
$ oc exec <any_es_pod_in_the_cluster> -c elasticsearch -- es_util --
query=_cluster/health?pretty=true
```

注記

直前のコマンドで使用した Elasticsearch Pod でロールアウトを実行した場合、Pod は存在しなくなっているため、ここで新規 Pod 名が必要になります。

以下に例を示します。

```
$ oc exec elasticsearch-cdm-5ceex6ts-1-dcd6c4c7c-jpw6 -c elasticsearch -- es_util --
query=_cluster/health?pretty=true
```

```
{
  "cluster_name" : "elasticsearch",
  "status" : "yellow", (1)
  "timed_out" : false,
```

```
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 8,
  "active_shards" : 16,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 1,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

1 次に進む前に、このパラメーターが **green** または **yellow** であることを確認します。

6. Elasticsearch 設定マップを変更した場合、それぞれの Elasticsearch Pod についてこれらの手順を繰り返します。

7. クラスターのすべてのデプロイメントがロールアウトされたら、シャードのバランシングを再度有効にします。

```
$ oc exec <any_es_pod_in_the_cluster> -c elasticsearch -- es_util --
query="_cluster/settings" -XPUT -d '{ "persistent": { "cluster.routing.allocation.enable" : "all" }
}'
```

以下に例を示します。

```
$ oc exec elasticsearch-cdm-5ceex6ts-1-dcd6c4c7c-jpw6 -c elasticsearch -- es_util --
query="_cluster/settings" -XPUT -d '{ "persistent": { "cluster.routing.allocation.enable" : "all" }
}'
```

出力例

```
{
  "acknowledged" : true,
  "persistent" : { },
  "transient" : {
    "cluster" : {
      "routing" : {
        "allocation" : {
          "enable" : "all"
        }
      }
    }
  }
}
```

3.3.9. ログストアサービスのルートとしての公開

デフォルトでは、クラスターロギングでデプロイされたログストアはロギングクラスターの外部からアクセスできません。データにアクセスするツールについては、ログストアへの外部アクセスのために re-encryption termination でルートを有効にすることができます。

re-encrypt ルート、OpenShift Container Platform トークンおよびインストールされたログストア CA 証明書を作成して、ログストアに外部からアクセスすることができます。次に、以下を含む cURL 要求でログストアサービスをホストするノードにアクセスします。

- **Authorization: Bearer ${token}**
- Elasticsearch reencrypt ルートおよび Elasticsearch API 要求

内部からは、ログストアクラスター IP を使用してログストアサービスにアクセスできます。これは、以下のコマンドのいずれかを使用して取得できます。

```
$ oc get service elasticsearch -o jsonpath={.spec.clusterIP} -n openshift-logging
```

出力例

```
172.30.183.229
```

```
$ oc get service elasticsearch -n openshift-logging
```

出力例

```
NAME            TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)    AGE
elasticsearch   ClusterIP   172.30.183.229   <none>        9200/TCP   22h
```

以下のようなコマンドを使用して、クラスター IP アドレスを確認できます。

```
$ oc exec elasticsearch-cdm-oplnhinv-1-5746475887-fj2f8 -n openshift-logging -- curl -tlsv1.2 --
insecure -H "Authorization: Bearer ${token}" "https://172.30.183.229:9200/_cat/health"
```

出力例

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    29  100    29    0     0    108      0 --:--:-- --:--:-- --:--:--   108
```

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。
- ログにアクセスできるようになるには、プロジェクトへのアクセスが必要です。

手順

ログストアを外部に公開するには、以下を実行します。

1. **openshift-logging** プロジェクトに切り替えます。

   ```
   $ oc project openshift-logging
   ```

2. ログストアから CA 証明書を抽出し、**admin-ca** ファイルに書き込みます。

   ```
   $ oc extract secret/elasticsearch --to=. --keys=admin-ca
   ```

出力例

```
admin-ca
```

3. ログストアサービスのルートを YAML ファイルとして作成します。

   a. 以下のように YAML ファイルを作成します。

```
apiVersion: route.openshift.io/v1
kind: Route
metadata:
  name: elasticsearch
  namespace: openshift-logging
spec:
  host:
  to:
    kind: Service
    name: elasticsearch
  tls:
    termination: reencrypt
    destinationCACertificate: | 1
```

   1 次の手順でログストア CA 証明書を追加するか、またはコマンドを使用します。一部の re-encrypt ルートで必要とされる **spec.tls.key**、**spec.tls.certificate**、および **spec.tls.caCertificate** パラメーターを設定する必要はありません。

   b. 以下のコマンドを実行して、作成したルート YAML にログストア CA 証明書を追加します。

```
$ cat ./admin-ca | sed -e "s/^/      /" >> <file-name>.yaml
```

   c. ルートを作成します。

```
$ oc create -f <file-name>.yaml
```

   出力例

```
route.route.openshift.io/elasticsearch created
```

4. Elasticsearch サービスが公開されていることを確認します。

   a. 要求に使用されるこのサービスアカウントのトークンを取得します。

```
$ token=$(oc whoami -t)
```

   b. 作成した **elasticsearch** ルートを環境変数として設定します。

```
$ routeES=`oc get route elasticsearch -o jsonpath={.spec.host}`
```

   c. ルートが正常に作成されていることを確認するには、公開されたルート経由で Elasticsearch にアクセスする以下のコマンドを実行します。

```
curl -tlsv1.2 --insecure -H "Authorization: Bearer ${token}" "https://${routeES}"
```

以下のような出力が表示されます。

出力例

```
{
  "name" : "elasticsearch-cdm-i40ktba0-1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "0eY-tJzcR3KOdpgeMJo-MQ",
  "version" : {
  "number" : "6.8.1",
  "build_flavor" : "oss",
  "build_type" : "zip",
  "build_hash" : "Unknown",
  "build_date" : "Unknown",
  "build_snapshot" : true,
  "lucene_version" : "7.7.0",
  "minimum_wire_compatibility_version" : "5.6.0",
  "minimum_index_compatibility_version" : "5.0.0"
},
  "<tagline>" : "<for search>"
}
```

3.4. ログビジュアライザーの設定

OpenShift Container Platform は Kibana を使用してクラスターロギングで収集されるログデータを表示します。

冗長性を確保するために Kibana をスケーリングし、Kibana ノードの CPU およびメモリーを設定することができます。

3.4.1. CPU およびメモリー制限の設定

クラスターロギングコンポーネントは、CPU とメモリーの制限の両方への調整を許可します。

手順

1. **openshift-logging** プロジェクトで **ClusterLogging** カスタムリソース (CR) を編集します。

```
$ oc edit ClusterLogging instance -n openshift-logging
```

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"

....

spec:
  managementState: "Managed"
  logStore:
    type: "elasticsearch"
```

```
  elasticsearch:
    nodeCount: 2
    resources: 1
      limits:
        memory: 2Gi
      requests:
        cpu: 200m
        memory: 2Gi
    storage:
      storageClassName: "gp2"
      size: "200G"
    redundancyPolicy: "SingleRedundancy"
  visualization:
    type: "kibana"
    kibana:
      resources: 2
        limits:
          memory: 1Gi
        requests:
          cpu: 500m
          memory: 1Gi
      proxy:
        resources: 3
          limits:
            memory: 100Mi
          requests:
            cpu: 100m
            memory: 100Mi
      replicas: 2
  curation:
    type: "curator"
    curator:
      resources: 4
        limits:
          memory: 200Mi
        requests:
          cpu: 200m
          memory: 200Mi
      schedule: "*/10 * * * *"
  collection:
    logs:
      type: "fluentd"
      fluentd:
        resources: 5
          limits:
            memory: 736Mi
          requests:
            cpu: 200m
            memory: 736Mi
```

1 必要に応じてログの CPU およびメモリーの制限および要求を指定します。Elasticsearch の場合、要求値と制限値の両方を調整する必要があります。

2 3 必要に応じて、ログビジュアライザーの CPU およびメモリーの制限および要求を指定します。

4 必要に応じて、ログキュレーターの CPU およびメモリーの制限および要求を指定します。

5 必要に応じて、ログコレクターの CPU およびメモリーの制限および要求を指定します。

3.4.2. ログビジュアライザーノードの冗長性のスケーリング

冗長性を確保するために、ログビジュアライザーをホストする Pod をスケーリングできます。

手順

1. **openshift-logging** プロジェクトで **ClusterLogging** カスタムリソース (CR) を編集します。

```
$ oc edit ClusterLogging instance
```

```
$ oc edit ClusterLogging instance

apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"

....

spec:
    visualization:
      type: "kibana"
      kibana:
        replicas: 1 (1)
```

1 Kibana ノードの数を指定します。

3.4.3. 容認を使用したログビジュアライザー Pod の配置の制御

ログビジュアライザー Pod が実行されるノードを制御し、Pod の容認を使用して他のワークロードがそれらのノードを使用しないようにすることができます。

ClusterLogging カスタムリソース (CR) を使用して容認をログビジュアライザー Pod に適用し、テイントをノード仕様でノードに適用します。ノードのテイントは、テイントを容認しないすべての Pod を拒否するようノードに指示する **key:value pair** です。他の Pod にはない特定の **key:value** ペアを使用することで、Kibana Pod のみをそのノード上で実行できます。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

1. 以下のコマンドを使用して、ログビジュアライザー Pod をスケジュールする必要のあるノードにテイントを追加します。

```
$ oc adm taint nodes <node-name> <key>=<value>:<effect>
```

以下に例を示します。

```
$ oc adm taint nodes node1 kibana=node:NoExecute
```

この例では、テイントをキー **kibana**、値 **node**、およびテイントの効果 **NoExecute** のある **node1** に配置します。**NoExecute** テイント effect を使用する必要があります。**NoExecute** は、テイントに一致する Pod のみをスケジュールし、一致しない既存の Pod を削除します。

2. **ClusterLogging** CR の **visualization** セクションを編集し、Kibana Pod の容認を設定します。

```
visualization:
  type: "kibana"
  kibana:
    tolerations:
    - key: "kibana" 1
      operator: "Exists" 2
      effect: "NoExecute" 3
      tolerationSeconds: 6000 4
```

1. ノードに追加したキーを指定します。
2. **Exists** Operator を指定して、**key/value/effect** パラメーターが一致するようにします。
3. **NoExecute** effect を指定します。
4. オプションで、**tolerationSeconds** パラメーターを指定して、エビクトされる前に Pod がノードにバインドされる期間を設定します。

この容認は、**oc adm taint** コマンドで作成されたテイントと一致します。この容認のある Pod は、**node1** にスケジュールできます。

3.5. クラスターロギングストレージの設定

Elasticsearch はメモリー集約型アプリケーションです。デフォルトのクラスターロギングインストールでは、メモリー要求およびメモリー制限の両方に対して 16G のメモリーをデプロイします。初期設定の OpenShift Container Platform ノードのセットは、Elasticsearch クラスターをサポートするのに十分な大きさではない場合があります。その場合、推奨されるサイズ以上のメモリーを使用して実行できるようにノードを OpenShift Container Platform クラスターに追加する必要があります。各 Elasticsearch ノードはこれより低い値のメモリー設定でも動作しますが、これは実稼働環境には推奨されません。

3.5.1. クラスターロギングおよび OpenShift Container Platform のストレージについての考慮事項

永続ボリュームは、それぞれの Elasticsearch デプロイメントに 1 つのデータノードに対して 1 つのデータボリュームを持たせるために必要です。OpenShift Container Platform では、これは永続ボリューム要求 (PVC) を使用して実行されます。

Elasticsearch Operator は Elasticsearch リソース名を使って PVC に名前を付けます。詳細は、永続 Elasticsearch ストレージを参照してください。

注記

永続ストレージにローカルボリュームを使用する場合は、**LocalVolume** オブジェクトの **volumeMode: block** で記述される raw ブロックボリュームを使用しないでください。Elasticsearch は raw ブロックボリュームを使用できません。

Fluentd は **systemd ジャーナル** および **/var/log/containers/** から Elasticsearch にログを送信します。

このため、必要なデータ量とアプリケーションログデータの集計方法を事前に検討しておく必要があります。一部の Elasticsearch ユーザーは、絶対的なストレージ使用率をおよそ 50% に維持し、常に 70% 未満にする必要があることを確認しています。これは、大規模なマージ操作を実行する際に Elasticsearch が応答しなくなる状態を避けるのに役立ちます。

デフォルトでは、85% になると Elasticsearch は新規データのノードへの割り当てを停止し、90% になると Elasticsearch は可能な場合に、該当ノードから別のノードへ既存シャードの移動を試行します。ただし、85% 未満の空き容量を持つノードがない場合、Elasticsearch は新規インデックスの作成を拒否し、ステータスは RED になります。

注記

これらの基準値 (高い値および低い値を含む) は現行リリースにおける Elasticsearch のデフォルト値です。これらの値を変更することはできますが、いずれの変更もアラートにも適用する必要があります。アラートはこれらのデフォルト値に基づくものです。

3.5.2. 追加リソース

- 永続的な Elasticsearch ストレージ

3.6. クラスターロギングコンポーネントの CPU およびメモリー制限の設定

必要に応じて、それぞれのクラスターロギングコンポーネントの CPU およびメモリー制限の両方を設定できます。

3.6.1. CPU およびメモリー制限の設定

クラスターロギングコンポーネントは、CPU とメモリーの制限の両方への調整を許可します。

手順

1. **openshift-logging** プロジェクトで **ClusterLogging** カスタムリソース (CR) を編集します。

```
$ oc edit ClusterLogging instance -n openshift-logging
```

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"

....

spec:
  managementState: "Managed"
  logStore:
```

```
  type: "elasticsearch"
  elasticsearch:
    nodeCount: 2
    resources: 1
      limits:
        memory: 2Gi
      requests:
        cpu: 200m
        memory: 2Gi
    storage:
      storageClassName: "gp2"
      size: "200G"
    redundancyPolicy: "SingleRedundancy"
visualization:
  type: "kibana"
  kibana:
    resources: 2
      limits:
        memory: 1Gi
      requests:
        cpu: 500m
        memory: 1Gi
    proxy:
      resources: 3
        limits:
          memory: 100Mi
        requests:
          cpu: 100m
          memory: 100Mi
    replicas: 2
curation:
  type: "curator"
  curator:
    resources: 4
      limits:
        memory: 200Mi
      requests:
        cpu: 200m
        memory: 200Mi
    schedule: "*/10 * * * *"
collection:
  logs:
    type: "fluentd"
    fluentd:
      resources: 5
        limits:
          memory: 736Mi
        requests:
          cpu: 200m
          memory: 736Mi
```

1 必要に応じてログの CPU およびメモリーの制限および要求を指定します。Elasticsearch の場合、要求値と制限値の両方を調整する必要があります。

2 3

必要に応じて、ログビジュアライザーの CPU およびメモリーの制限および要求を指定します。

4 必要に応じて、ログキュレーターの CPU およびメモリーの制限および要求を指定します。

5 必要に応じて、ログコレクターの CPU およびメモリーの制限および要求を指定します。

3.7. 容認を使用した クラスターロギング POD 配置の制御

テイントおよび容認を使用することで、クラスターロギング Pod が特定のノードで実行され、その他のワークロードがそれらのノードで実行されないようにします。

テイントおよび容認は、単純な **key:value** のペアです。ノードのテイントはノードに対し、テイントを容認しないすべての Pod を拒否するよう指示します。

key は最大 253 文字までの文字列で、 **value** は最大 63 文字までの文字列になります。文字列は文字または数字で開始する必要があり、文字、数字、ハイフン、ドットおよびアンダースコアを含めることができます。

容認を使用したクラスターロギング CR のサンプル

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"
  namespace: openshift-logging
spec:
  managementState: "Managed"
  logStore:
    type: "elasticsearch"
    elasticsearch:
      nodeCount: 1
      tolerations: 1
      - key: "logging"
        operator: "Exists"
        effect: "NoExecute"
        tolerationSeconds: 6000
      resources:
        limits:
          memory: 8Gi
        requests:
          cpu: 100m
          memory: 1Gi
      storage: {}
      redundancyPolicy: "ZeroRedundancy"
  visualization:
    type: "kibana"
    kibana:
      tolerations: 2
      - key: "logging"
        operator: "Exists"
        effect: "NoExecute"
        tolerationSeconds: 6000
```

```
      resources:
        limits:
          memory: 2Gi
        requests:
          cpu: 100m
          memory: 1Gi
      replicas: 1
  collection:
    logs:
      type: "fluentd"
      fluentd:
        tolerations: 3
        - key: "logging"
          operator: "Exists"
          effect: "NoExecute"
          tolerationSeconds: 6000
        resources:
          limits:
            memory: 2Gi
          requests:
            cpu: 100m
            memory: 1Gi
```

1 この容認は Elasticsearch Pod に追加されます。

2 この容認は Kibana Pod に追加されます。

3 この容認はロギングコレクター Pod に追加されます。

3.7.1. 容認を使用したログストア Pod の配置の制御

ログストア Pod が実行するノードを制御し、Pod の容認を使用して他のワークロードがそれらのノードを使用しないようにすることができます。

ClusterLogging カスタムリソース (CR) を使用して容認をログストア Pod に適用し、テイントをノード仕様でノードに適用します。ノードのテイントは、テイントを容認しないすべての Pod を拒否するようノードに指示する **key:value pair** です。他の Pod にはない特定の **key:value** ペアを使用することで、ログストア Pod のみがそのノード上で実行されるようにできます。

デフォルトで、ログストア Pod には以下の容認があります。

```
tolerations:
- effect: "NoExecute"
  key: "node.kubernetes.io/disk-pressure"
  operator: "Exists"
```

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

1. 以下のコマンドを使用して、クラスターロギング Pod をスケジュールするノードにテイントを追加します。

```
$ oc adm taint nodes <node-name> <key>=<value>:<effect>
```

以下は例になります。

```
$ oc adm taint nodes node1 elasticsearch=node:NoExecute
```

この例では、テイントをキー **elasticsearch**、値 **node**、およびテイントの効果 **NoExecute** のある **node1** に配置します。**NoExecute** effect のノードは、テイントに一致する Pod のみをスケジュールし、一致しない既存の Pod を削除します。

2. **ClusterLogging** CR の **logstore** セクションを編集し、Elasticsearch Pod の容認を設定します。

```
logStore:
  type: "elasticsearch"
  elasticsearch:
    nodeCount: 1
    tolerations:
    - key: "elasticsearch" (1)
      operator: "Exists" (2)
      effect: "NoExecute" (3)
      tolerationSeconds: 6000 (4)
```

(1) ノードに追加したキーを指定します。

(2) **Exists** Operator を指定し、キー **elasticsearch** のあるテイントがノードに存在する必要があるようにします。

(3) **NoExecute** effect を指定します。

(4) オプションで、**tolerationSeconds** パラメーターを指定して、エビクトされる前に Pod がノードにバインドされる期間を設定します。

この容認は、**oc adm taint** コマンドで作成されたテイントと一致します。この容認のある Pod は **node1** にスケジュールできます。

3.7.2. 容認を使用したログビジュアライザー Pod の配置の制御

ログビジュアライザー Pod が実行されるノードを制御し、Pod の容認を使用して他のワークロードがそれらのノードを使用しないようにすることができます。

ClusterLogging カスタムリソース (CR) を使用して容認をログビジュアライザー Pod に適用し、テイントをノード仕様でノードに適用します。ノードのテイントは、テイントを容認しないすべての Pod を拒否するようノードに指示する **key:value pair** です。他の Pod にはない特定の **key:value** ペアを使用することで、Kibana Pod のみをそのノード上で実行できます。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

1. 以下のコマンドを使用して、ログビジュアライザー Pod をスケジュールする必要のあるノードにテイントを追加します。

```
$ oc adm taint nodes <node-name> <key>=<value>:<effect>
```

以下に例を示します。

```
$ oc adm taint nodes node1 kibana=node:NoExecute
```

この例では、テイントをキー **kibana**、値 **node**、およびテイントの効果 **NoExecute** のある **node1** に配置します。**NoExecute** テイント effect を使用する必要があります。**NoExecute** は、テイントに一致する Pod のみをスケジュールし、一致しない既存の Pod を削除します。

2. **ClusterLogging** CR の **visualization** セクションを編集し、Kibana Pod の容認を設定します。

```
visualization:
  type: "kibana"
  kibana:
    tolerations:
    - key: "kibana" 1
      operator: "Exists" 2
      effect: "NoExecute" 3
      tolerationSeconds: 6000 4
```

1. ノードに追加したキーを指定します。
2. **Exists** Operator を指定して、**key/value/effect** パラメーターが一致するようにします。
3. **NoExecute** effect を指定します。
4. オプションで、**tolerationSeconds** パラメーターを指定して、エビクトされる前に Pod がノードにバインドされる期間を設定します。

この容認は、**oc adm taint** コマンドで作成されたテイントと一致します。この容認のある Pod は、**node1** にスケジュールできます。

3.7.3. 容認を使用したログコレクター Pod 配置の制御

ロギングコレクター Pod が実行するノードを確認し、Pod の容認を使用して他のワークロードがそれらのノードを使用しないようにすることができます。

容認を **ClusterLogging** カスタムリソース (CR) でロギングコレクター Pod に適用し、テイントをノード仕様でノードに適用します。テイントおよび容認を使用すると、Pod がメモリーや CPU などの問題によってエビクトされないようにすることができます。

デフォルトで、ロギングコレクター Pod には以下の容認があります。

```
tolerations:
- key: "node-role.kubernetes.io/master"
  operator: "Exists"
  effect: "NoExecute"
```

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

1. 以下のコマンドを使用して、ロギングコレクター Pod がロギングコレクター Pod をスケジュールする必要のあるノードにテイントを追加します。

```
$ oc adm taint nodes <node-name> <key>=<value>:<effect>
```

以下に例を示します。

```
$ oc adm taint nodes node1 collector=node:NoExecute
```

この例では、テイントをキー **collector**、値 **node**、およびテイント effect **NoExecute** のある **node1** に配置します。**NoExecute** テイント effect を使用する必要があります。**NoExecute** は、テイントに一致する Pod のみをスケジュールし、一致しない既存の Pod を削除します。

2. **ClusterLogging** カスタムリソース (CR) の **collection** スタンザを編集して、ロギングコレクター Pod の容認を設定します。

```
collection:
  logs:
    type: "fluentd"
    fluentd:
      tolerations:
      - key: "collector" (1)
        operator: "Exists" (2)
        effect: "NoExecute" (3)
        tolerationSeconds: 6000 (4)
```

(1) ノードに追加したキーを指定します。

(2) **Exists** Operator を指定して、**key/value/effect** パラメーターが一致するようにします。

(3) **NoExecute** effect を指定します。

(4) オプションで、**tolerationSeconds** パラメーターを指定して、エビクトされる前に Pod がノードにバインドされる期間を設定します。

この容認は、**oc adm taint** コマンドで作成されたテイントと一致します。この容認のある Pod は、**node1** にスケジュールできます。

3.7.4. 追加リソース

テイントおよび容認についての詳細は、ノードテイントを使用した Pod 配置の制御 を参照してください。

3.8. ノードセレクターを使用したクラスターロギングリソースの移動

ノードセレクターを使用して Elasticsearch、Kibana、Curator Pod を異なるノードにデプロイすることができます。

3.8.1. クラスターロギングリソースの移動

すべてのクラスターロギングコンポーネント、Elasticsearch、Kibana、および Curator の Pod を異なるノードにデプロイするように Cluster Logging Operator を設定できます。Cluster Logging Operator Pod については、インストールされた場所から移動することはできません。

たとえば、Elasticsearch Pod の CPU、メモリーおよびディスクの要件が高いために、この Pod を別のノードに移動できます。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。これらの機能はデフォルトでインストールされません。

手順

1. **openshift-logging** プロジェクトで **ClusterLogging** カスタムリソース (CR) を編集します。

```
$ oc edit ClusterLogging instance
```

```
apiVersion: logging.openshift.io/v1
kind: ClusterLogging

...

spec:
  collection:
    logs:
      fluentd:
        resources: null
      type: fluentd
  curation:
    curator:
      nodeSelector: 1
        node-role.kubernetes.io/infra: ''
      resources: null
      schedule: 30 3 * * *
    type: curator
  logStore:
    elasticsearch:
      nodeCount: 3
      nodeSelector: 2
        node-role.kubernetes.io/infra: ''
      redundancyPolicy: SingleRedundancy
      resources:
        limits:
          cpu: 500m
          memory: 16Gi
        requests:
          cpu: 500m
          memory: 16Gi
      storage: {}
    type: elasticsearch
  managementState: Managed
  visualization:
```

```
    kibana:
      nodeSelector: 3
        node-role.kubernetes.io/infra: ''
      proxy:
        resources: null
      replicas: 1
      resources: null
    type: kibana

...
```

1 2 3 適切な値が設定された **nodeSelector** パラメーターを、移動する必要のあるコンポーネントに追加します。表示されている形式の **nodeSelector** を使用することも、ノードに指定された値に基づいて **<key>: <value>** ペアを使用することもできます。

検証

コンポーネントが移動したことを確認するには、**oc get pod -o wide** コマンドを使用できます。

以下に例を示します。

- Kibana Pod を **ip-10-0-147-79.us-east-2.compute.internal** ノードから移動する必要がある場合、以下を実行します。

```
$ oc get pod kibana-5b8bdf44f9-ccpq9 -o wide
```

出力例

```
NAME                     READY   STATUS    RESTARTS   AGE   IP            NODE
NOMINATED NODE   READINESS GATES
kibana-5b8bdf44f9-ccpq9  2/2     Running   0          27s   10.129.2.18   ip-10-0-147-79.us-
east-2.compute.internal   <none>           <none>
```

- Kibana Pod を、専用インフラストラクチャーノードである **ip-10-0-139-48.us-east-2.compute.internal** ノードに移動する必要がある場合、以下を実行します。

```
$ oc get nodes
```

出力例

```
NAME                                         STATUS   ROLES          AGE   VERSION
ip-10-0-133-216.us-east-2.compute.internal   Ready    master         60m   v1.18.3
ip-10-0-139-146.us-east-2.compute.internal   Ready    master         60m   v1.18.3
ip-10-0-139-192.us-east-2.compute.internal   Ready    worker         51m   v1.18.3
ip-10-0-139-241.us-east-2.compute.internal   Ready    worker         51m   v1.18.3
ip-10-0-147-79.us-east-2.compute.internal    Ready    worker         51m   v1.18.3
ip-10-0-152-241.us-east-2.compute.internal   Ready    master         60m   v1.18.3
ip-10-0-139-48.us-east-2.compute.internal    Ready    infra          51m   v1.18.3
```

ノードには **node-role.kubernetes.io/infra: ''** ラベルがあることに注意してください。

```
$ oc get node ip-10-0-139-48.us-east-2.compute.internal -o yaml
```

出力例

```
kind: Node
apiVersion: v1
metadata:
  name: ip-10-0-139-48.us-east-2.compute.internal
  selfLink: /api/v1/nodes/ip-10-0-139-48.us-east-2.compute.internal
  uid: 62038aa9-661f-41d7-ba93-b5f1b6ef8751
  resourceVersion: '39083'
  creationTimestamp: '2020-04-13T19:07:55Z'
  labels:
    node-role.kubernetes.io/infra: ''
...
```

- Kibana Pod を移動するには、**ClusterLogging** CR を編集してノードセレクターを追加します。

```
apiVersion: logging.openshift.io/v1
kind: ClusterLogging

...

spec:

...

  visualization:
    kibana:
      nodeSelector: 1
        node-role.kubernetes.io/infra: ''
      proxy:
        resources: null
      replicas: 1
      resources: null
    type: kibana
```

1 ノード仕様のラベルに一致するノードセレクターを追加します。

- CR を保存した後に、現在の Kibana Pod は終了し、新規 Pod がデプロイされます。

```
$ oc get pods
```

出力例

```
NAME                                            READY   STATUS      RESTARTS   AGE
cluster-logging-operator-84d98649c4-zb9g7       1/1     Running     0          29m
elasticsearch-cdm-hwv01pf7-1-56588f554f-kpmlg   2/2     Running     0          28m
elasticsearch-cdm-hwv01pf7-2-84c877d75d-75wqj   2/2     Running     0          28m
elasticsearch-cdm-hwv01pf7-3-f5d95b87b-4nx78    2/2     Running     0          28m
fluentd-42dzz                                   1/1     Running     0          28m
fluentd-d74rq                                   1/1     Running     0          28m
fluentd-m5vr9                                   1/1     Running     0          28m
fluentd-nkxl7                                   1/1     Running     0          28m
fluentd-pdvqb                                   1/1     Running     0          28m
```

```
fluentd-tflh6                           1/1     Running       0          28m
kibana-5b8bdf44f9-ccpq9                 2/2     Terminating   0          4m11s
kibana-7d85dcffc8-bfpfp                 2/2     Running       0          33s
```

- 新規 Pod が **ip-10-0-139-48.us-east-2.compute.internal** ノードに置かれます。

```
$ oc get pod kibana-7d85dcffc8-bfpfp -o wide
```

出力例

```
NAME                     READY   STATUS       RESTARTS   AGE   IP          NODE
NOMINATED NODE   READINESS GATES
kibana-7d85dcffc8-bfpfp   2/2     Running      0          43s   10.131.0.22   ip-10-0-139-48.us-
east-2.compute.internal   <none>           <none>
```

- しばらくすると、元の Kibana Pod が削除されます。

```
$ oc get pods
```

出力例

```
NAME                                READY   STATUS    RESTARTS   AGE
cluster-logging-operator-84d98649c4-zb9g7       1/1     Running   0          30m
elasticsearch-cdm-hwv01pf7-1-56588f554f-kpmlg   2/2     Running   0          29m
elasticsearch-cdm-hwv01pf7-2-84c877d75d-75wqj   2/2     Running   0          29m
elasticsearch-cdm-hwv01pf7-3-f5d95b87b-4nx78    2/2     Running   0          29m
fluentd-42dzz                           1/1     Running   0          29m
fluentd-d74rq                           1/1     Running   0          29m
fluentd-m5vr9                           1/1     Running   0          29m
fluentd-nkxl7                           1/1     Running   0          29m
fluentd-pdvqb                           1/1     Running   0          29m
fluentd-tflh6                           1/1     Running   0          29m
kibana-7d85dcffc8-bfpfp                 2/2     Running   0          62s
```

3.9. SYSTEMD-JOURNALD および FLUENTD の設定

Fluentd のジャーナルからの読み取りや、ジャーナルのデフォルト設定値は非常に低く、ジャーナルがシステムサービスからのロギング速度に付いていくことができないためにジャーナルエントリーが失われる可能性があります。

ジャーナルでエントリーが失われるのを防ぐことができるように **RateLimitInterval=1s** および **RateLimitBurst=10000** (必要な場合はさらに高い値) を設定することが推奨されます。

3.9.1. クラスターロギング用の systemd-journald の設定

プロジェクトのスケールアップ時に、デフォルトのロギング環境にはいくらかの調整が必要になる場合があります。

たとえば、ログが見つからない場合は、journald の速度制限を引き上げる必要がある場合があります。一定期間保持するメッセージ数を調整して、クラスターロギングがログをドロップせずに過剰なリソースを使用しないようにすることができます。

また、ログを圧縮する必要があるかどうか、ログを保持する期間、ログを保存する方法、ログを保存するかどうかやその他の設定を決定することもできます。

手順

1. 必要な設定で **journald.conf** ファイルを作成します。

```
Compress=yes (1)
ForwardToConsole=no (2)
ForwardToSyslog=no
MaxRetentionSec=1month (3)
RateLimitBurst=10000 (4)
RateLimitInterval=1s
Storage=persistent (5)
SyncIntervalSec=1s (6)
SystemMaxUse=8g (7)
SystemKeepFree=20% (8)
SystemMaxFileSize=10M (9)
```

(1) ログがファイルシステムに書き込まれる前にそれらのログを圧縮するかどうかを指定します。**yes** を指定してメッセージを圧縮するか、または **no** を指定して圧縮しないようにします。デフォルトは **yes** です。

(2) ログメッセージを転送するかどうかを設定します。それぞれについて、デフォルトで **no** に設定されます。以下を指定します。

- **ForwardToConsole**: ログをシステムコンソールに転送します。
- **ForwardToKsmg**: ログをカーネルログバッファーに転送します。
- **ForwardToSyslog**: syslog デーモンに転送します。
- **ForwardToWall**: メッセージを wall メッセージとしてすべてのログインしているユーザーに転送します。

(3) ジャーナルエントリーを保存する最大時間を指定します。数字を入力して秒数を指定します。または、year、month、week、day、h または m などの単位を含めます。無効にするには **0** を入力します。デフォルトは **1month** です。

(4) レート制限を設定します。**RateLimitIntervalSec** で定義される期間に、 **RateLimitBurst** で指定される以上のログが受信される場合、この期間内の追加のメッセージすべてはこの期間が終了するまでにドロップされます。デフォルト値である **RateLimitInterval=1s** および **RateLimitBurst=10000** を設定することが推奨されます。

(5) ログの保存方法を指定します。デフォルトは **persistent** です。

- **volatile**: ログを **/var/log/journal/** のメモリーに保存します。
- **persistent**: ログを **/var/log/journal/** のディスクに保存します。systemd は存在しない場合はディレクトリーを作成します。
- **auto**: ディレクトリーが存在する場合に、ログを **/var/log/journal/** に保存します。存在しない場合は、systemd はログを **/run/systemd/journal** に一時的に保存します。
- **none**: ログを保存しません。systemd はすべてのログをドロップします。

6 **ERR**、**WARNING**、**NOTICE**、**INFO**、および **DEBUG** ログについてジャーナルファイルをディスクに同期させるまでのタイムアウトを指定します。 systemd は、**CRIT**、**ALERT**、

7 ジャーナルが使用できる最大サイズを指定します。デフォルトは **8g** です。

8 systemd が残す必要のあるディスク領域のサイズを指定します。デフォルトは **20%** です。

9 **/var/log/journal** に永続的に保存される個別のジャーナルファイルの最大サイズを指定します。デフォルトは **10M** です。

注記

レート制限を削除する場合、システムロギングデーモンの CPU 使用率が高くなることがあります。 以前はスロットリングされていた可能性のあるメッセージが処理されるためです。

systemd 設定の詳細については、https://www.freedesktop.org/software/systemd/man/journald.conf.html を参照してください。このページに一覧表示されるデフォルト設定は OpenShift Container Platform には適用されない可能性があります。

2. **journal.conf** ファイルを base64 に変換します。

```
$ export jrnl_cnf=$( cat /journald.conf | base64 -w0 )
```

3. マスターまたはワーカー用に新規の **MachineConfig** を作成し、 **journal.conf** パラメーターを追加します。
以下は例になります。

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: worker
  name: 50-corp-journald
spec:
  config:
    ignition:
      version: 2.2.0
    storage:
      files:
      - contents:
          source: data:text/plain;charset=utf-8;base64,${jrnl_cnf}
        mode: 0644 1
        overwrite: true
        path: /etc/systemd/journald.conf 2
```

1 **journal.conf** ファイルのパーミッションを設定します。**0644** パーミッションを設定することが推奨されます。

2 base64 でエンコードされた **journal.conf** ファイルへのパスを指定します。

4. マシン設定を作成します。

```
$ oc apply -f <filename>.yaml
```

コントローラーは新規の **MachineConfig** オブジェクトを検出し、新規の **rendered-worker-<hash>** バージョンを生成します。

5. 新規のレンダリングされた設定の各ノードへのロールアウトのステータスをモニターします。

```
$ oc describe machineconfigpool/worker
```

出力例

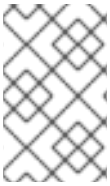
```
Name:         worker
Namespace:
Labels:       machineconfiguration.openshift.io/mco-built-in=
Annotations:  <none>
API Version:  machineconfiguration.openshift.io/v1
Kind:         MachineConfigPool

...

Conditions:
  Message:
  Reason:               All nodes are updating to rendered-worker-
913514517bcea7c93bd446f4830bc64e
```

3.10. ログキュレーターの設定

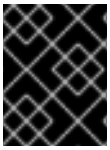
ログの保持時間を設定することができます。デフォルトの Elasticsearch ログストアが、インフラストラクチャーログ、アプリケーションログ、監査ログなどの 3 つのログソースごとに個別の保持ポリシーを設定してインデックスを保持する期間を指定できます。手順については、ログ保持時間の設定 について参照してください。



注記

ログデータのキュレーションには、ログ保持時間を設定することが推奨されます。これは、現在のデータモデルと OpenShift Container Platform 4.4 以前のバージョンの以前のデータモデルの両方で機能します。

オプションで、OpenShift Container Platform 4.4 以前からデータモデルを使用する Elasticsearch インデックスを削除するには、Elasticsearch Curator を使用することもできます。以下のセクションでは、Elasticsearch Curator を使用する方法について説明します。

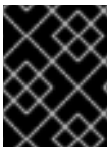


重要

Elasticsearch Curator は OpenShift Container Platform 4.7 (OpenShift Logging 5.0) で非推奨となり、OpenShift Logging 5.1 で削除されます。

3.10.1. Curator スケジュールの設定

OpenShift Logging インストールで作成された **Cluster Logging** カスタムリソースを使用して、Curator のスケジュールを指定できます。



重要

Elasticsearch Curator は OpenShift Container Platform 4.7 (OpenShift Logging 5.0) で非推奨となり、OpenShift Logging 5.1 で削除されます。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

Curator スケジュールを設定するには、以下を実行します。

1. **openshift-logging** プロジェクトで **ClusterLogging** カスタムリソースを編集します。

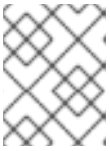
```
$ oc edit clusterlogging instance
```

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"

...

  curation:
    curator:
      schedule: 30 3 * * * 1
    type: curator
```

1 Curator のスケジュールを cron 形式 で指定します。



注記

タイムゾーンは Curator Pod が実行されるホストノードに基づいて設定されます。

3.10.2. Curator インデックス削除の設定

OpenShift Container Platform バージョン 4.5 よりも前のデータモデルを使用する Elasticsearch データを削除するように Elasticsearch Curator を設定できます。プロジェクトごとの設定およびグローバル設定を行うことができます。グローバル設定は、指定されていないプロジェクトに適用されます。プロジェクトごとの設定はグローバル設定を上書きします。

重要

Elasticsearch Curator は OpenShift Container Platform 4.7 (OpenShift Logging 5.0) で非推奨となり、OpenShift Logging 5.1 で削除されます。

前提条件

- クラスターロギングがインストールされている必要があります。

手順

インデックスを削除するには、以下を実行します。

1. OpenShift Container Platform カスタム Curator 設定ファイルを編集します。

```
$ oc edit configmap/curator
```

2. 必要に応じて以下のパラメーターを設定します。

```
config.yaml: |
  project_name:
    action
      unit:value
```

利用可能なパラメーターを以下に示します。

表3.2 プロジェクトオプション

変数名	説明
project_name	プロジェクトの実際の名前 (**myapp-devel** など)。OpenShift Container Platform の**操作**ログについては、名前 **.operations** をプロジェクト名として使用します。
action	実行するアクション。現在許可されているのは **delete** のみです。
unit	削除に使用する期間 (**days**、**weeks**、または **months**)。
value	単位数。

表3.3 フィルターオプション

変数名	説明
.defaults	**.defaults** を **project_name** として使用し、指定されていないプロジェクトのデフォルトを設定します。
.regex	プロジェクト名に一致する正規表現の一覧。
pattern	適切にエスケープされた有効な正規表現パターン。一重引用符で囲まれています。

たとえば、以下のように Curator を設定します。

- **1 day** を経過した **myapp-dev** プロジェクトのインデックスを削除する
- **1 week** を経過した **myapp-qe** プロジェクトのインデックスを削除する
- **8 weeks** を経過した **operations** ログを削除する
- **31 days** を経過したその他すべてのプロジェクトのインデックスを削除する

- **^project\..+\-dev.*$** 正規表現と一致する、1 日を経過したインデックスを削除する
- **^project\..+\-test.*$** 正規表現と一致する、2 日を経過したインデックスを削除する

以下を使用します。

```
config.yaml: |
  .defaults:
    delete:
      days: 31

  .operations:
    delete:
      weeks: 8

  myapp-dev:
    delete:
      days: 1

  myapp-qe:
    delete:
      weeks: 1

  .regex:
    - pattern: '^project\..+\-dev\..*$'
      delete:
        days: 1
    - pattern: '^project\..+\-test\..*$'
      delete:
        days: 2
```

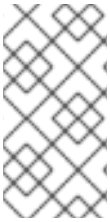
重要

months を操作の **$UNIT** として使用する場合、Curator は今月の当日ではなく、今月の最初の日からカウントを開始します。たとえば、今日が 4 月 15 日であり、現時点で 2 カ月を経過したインデックスを削除する場合 (delete: months: 2)、Curator は 2 月 15 日より古い日付のインデックスを削除するのではなく、2 月 1 日より古いインデックスを削除します。つまり、今月の最初の日付まで遡り、そこから 2 カ月遡ります。Curator で厳密な設定をする必要がある場合、最も適切な方法として日数 (例: **delete: days: 30**) を使用することができます。

3.11. メンテナーンスとサポート

3.11.1. サポートされる設定

クラスターロギングの設定のサポートされる方法として、本書で説明されているオプションを使用してこれを設定することができます。サポートされていない他の設定は使用しないでください。設定のパラダイムが OpenShift Container Platform リリース間で変更される可能性があり、このような変更は、設定のすべての可能性が制御されている場合のみ適切に対応できます。本書で説明されている設定以外の設定を使用する場合、Elasticsearch Operator および Cluster Logging Operator が差分を調整するため、変更内容は失われます。Operator はデフォルトで定義された状態にすべて戻します。



注記

OpenShift Container Platform ドキュメントで説明されていない設定を実行する **必要がある** 場合、Cluster Logging Operator または Elasticsearch Operator を **Unmanaged** (管理外) に設定する **必要があります**。管理外のクラスターロギング環境は **サポート対象外** であり、クラスターロギングを **Managed** に戻すまで変更を受信しません。

3.11.2. サポートされない設定

以下のコンポーネントを変更するには、Cluster Logging Operator を Unmanaged (管理外) の状態に設定する必要があります。

- Curator cron ジョブ
- **Elasticsearch** CR
- Kibana デプロイメント
- **fluent.conf** ファイル
- Fluentd デーモンセット

以下のコンポーネントを変更するには、Elasticsearch Operator を Unmanaged(管理外) の状態に設定する必要があります。

- Elasticsearch デプロイメントファイル。

明示的にサポート対象外とされているケースには、以下が含まれます。

- **デフォルトのログローテーションの設定**。デフォルトのログローテーション設定は変更できません。
- **収集したログの場所の設定**。ログコレクターの出力ファイルの場所を変更することはできません。デフォルトは **/var/log/fluentd/fluentd.log** です。
- **ログコレクションのスロットリング**。ログコレクターによってログが読み取られる速度を調整して減速することはできません。
- **ログコレクション JSON 解析の設定**。JSON でログメッセージをフォーマットすることはできません。
- **環境変数を使用したロギングコレクターの設定**。環境変数を使用してログコレクターを変更することはできません。
- **ログコレクターによってログを正規化する方法の設定**。デフォルトのログの正規化を変更することはできません。
- **スクリプト化されたデプロイメントでの Curator の設定**。スクリプト化されたデプロイメントでログ収集を設定することはできません。
- **Curator Action ファイルの使用**。Curator 設定マップを使用して Curator Action ファイルを変更することはできません。

3.11.3. 管理外の Operator のサポートポリシー

Operator の **管理状態** は、Operator が設計通りにクラスター内の関連するコンポーネントのリソースをアクティブに管理しているかどうかを定めます。Operator が **unmanaged** 状態に設定されている場合、これは設定の変更に応答せず、更新を受信しません。

これは非実稼働クラスターやデバッグ時に便利ですが、管理外の状態の Operator はサポートされず、クラスター管理者は個々のコンポーネント設定およびアップグレードを完全に制御していることを前提としています。

Operator は以下の方法を使用して管理外の状態に設定できます。

- **個別の Operator 設定**
  個別の Operator には、それらの設定に **managementState** パラメーターがあります。これは Operator に応じてさまざまな方法でアクセスできます。たとえば、Cluster Logging Operator は管理するカスタムリソース (CR) を変更することによってこれを実行しますが、Cluster Samples Operator はクラスター全体の設定リソースを使用します。

  managementState パラメーターを **Unmanaged** に変更する場合、Operator はそのリソースをアクティブに管理しておらず、コンポーネントに関連するアクションを取らないことを意味します。Operator によっては、クラスターが破損し、手動リカバリーが必要になる可能性があるため、この管理状態に対応しない可能性があります。

  警告

  個別の Operator を **Unmanaged** 状態に変更すると、特定のコンポーネントおよび機能がサポート対象外になります。サポートを継続するには、報告された問題を **Managed** 状態で再現する必要があります。

- **Cluster Version Operator (CVO) のオーバーライド**
  spec.overrides パラメーターを CVO の設定に追加すると、管理者はコンポーネントについての CVO の動作に対してオーバーライドの一覧を追加できます。コンポーネントについて **spec.overrides[].unmanaged** パラメーターを **true** に設定すると、クラスターのアップグレードがブロックされ、CVO のオーバーライドが設定された後に管理者にアラートが送信されます。

  > Disabling ownership via cluster version overrides prevents upgrades. Please remove overrides before continuing.

  警告

  CVO のオーバーライドを設定すると、クラスター全体がサポートされない状態になります。サポートを継続するには、オーバーライドを削除した後に、報告された問題を再現する必要があります。

第4章 リソースのログの表示

OpenShift CLI (oc) および Web コンソールを使用して、ビルド、デプロイメント、および Pod などの各種リソースのログを表示できます。

注記

リソースログは、制限されたログ表示機能を提供するデフォルトの機能です。ログの取得および表示のエクスペリエンスを強化するには、OpenShift Container Platform クラスターロギング をインストールすることが推奨されます。Cluster Logging は、ノードシステムの監査ログ、アプリケーションコンテナーログ、およびインフラストラクチャーログなどの OpenShift Container Platform クラスターからのすべてのログを専用のログストアに集計します。次に、Kibana インターフェイス を使用してログデータをクエリーし、検出し、可視化できます。リソースログはクラスターロギングのログストアにアクセスしません。

4.1. リソースログの表示

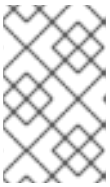
OpenShift CLI (oc) および Web コンソールで、各種リソースのログを表示できます。ログの末尾から読み取られるログ。

前提条件

- OpenShift CLI (oc) へのアクセス。

手順 (UI)

1. OpenShift Container Platform コンソールで **Workloads → Pods** に移動するか、または調査するリソースから Pod に移動します。



注記

ビルドなどの一部のリソースには、直接クエリーする Pod がありません。このような場合には、リソースについて **Details** ページで **Logs** リンクを特定できます。

2. ドロップダウンメニューからプロジェクトを選択します。
3. 調査する Pod の名前をクリックします。
4. **Logs** をクリックします。

手順 (CLI)

- 特定の Pod のログを表示します。

```
$ oc logs -f <pod_name> -c <container_name>
```

ここでは、以下のようになります。

-f
オプション: ログに書き込まれている内容に沿って出力することを指定します。

<pod_name>

Pod の名前を指定します。

<container_name>

オプション: コンテナーの名前を指定します。Pod に複数のコンテナーがある場合、コンテナー名を指定する必要があります。

以下に例を示します。

```
$ oc logs ruby-58cd97df55-mww7r
```

```
$ oc logs -f ruby-57f7f4855b-znl92 -c ruby
```

ログファイルの内容が出力されます。

- 特定のリソースのログを表示します。

```
$ oc logs <object_type>/<resource_name> 1
```

1 リソースタイプおよび名前を指定します。

以下に例を示します。

```
$ oc logs deployment/ruby
```

ログファイルの内容が出力されます。

第5章 KIBANA を使用したクラスターログの表示

OpenShift Container Platform クラスターロギングには、収集したログデータを視覚化するための Web コンソールが含まれます。現時点で、OpenShift Container Platform では、可視化できるように Kibana コンソールをデプロイします。

ログビジュアライザーを使用して、データで以下を実行できます。

- **Discover** タブを使用してデータを検索し、参照します。
- **Visualize** タブを使用してデータのグラフを表示し、データをマップします。
- **Dashboard** タブを使用してカスタムダッシュボードを作成し、表示します。

Kibana インターフェイスの使用および設定については、本書では扱いません。詳細については、Kibana ドキュメント を参照してください。

注記

監査ログは、デフォルトでは内部 OpenShift Container Platform Elasticsearch インスタンスに保存されません。Kibana で監査ログを表示するには、ログ転送 API を使用して、監査ログの **default** 出力を使用するパイプラインを設定する必要があります。

5.1. KIBANA インデックスパターンの定義

インデックスパターンは、可視化する必要のある Elasticsearch インデックスを定義します。Kibana でデータを確認し、可視化するには、インデックスパターンを作成する必要があります。

前提条件

- Kibana で **infra** および **audit** インデックスを表示するには、ユーザーには **cluster-admin** ロール、 **cluster-reader** ロール、または両方のロールが必要です。デフォルトの **kubeadmin** ユーザーには、これらのインデックスを表示するための適切なパーミッションがあります。**default**、**kube-** および **openshift-** プロジェクトで Pod およびログを表示できる場合、これらのインデックスにアクセスできるはずです。以下のコマンドを使用して、現在のユーザーが適切なパーミッションを持っているかどうかを確認することができます。

```
$ oc auth can-i get pods/log -n <project>
```

出力例

```
yes
```

注記

監査ログは、デフォルトでは内部 OpenShift Container Platform Elasticsearch インスタンスに保存されません。Kibana で監査ログを表示するには、ログ転送 API を使用して監査ログの **default** 出力を使用するパイプラインを設定する必要があります。

- Elasticsearch ドキュメントは、インデックスパターンを作成する前にインデックス化する必要があります。これは自動的に実行されますが、新規または更新されたクラスターでは数分の時間がかかる可能性があります。

手順

Kibana でインデックスパターンを定義し、ビジュアライゼーションを作成するには、以下を実行します。

1. OpenShift Container Platform コンソールで、Application Launcher  をクリックし、**Logging** を選択します。
2. **Management → Index Patterns → Create index pattern** をクリックして Kibana インデックスパターンを作成します。
   - 各ユーザーは、プロジェクトのログを確認するために、Kibana に初めてログインする際にインデックスパターンを手動で作成する必要があります。ユーザーは **app** という名前のインデックスパターンを作成し、**@timestamp** 時間フィールドを使用してコンテナーログを表示する必要があります。
   - 管理ユーザーはそれぞれ、最初に Kibana にログインする際に、**@timestamp** 時間フィールドを使用して **app**、 **infra** および **audit** インデックスについてインデックスパターンを作成する必要があります。
3. 新規インデックスパターンから Kibana のビジュアライゼーション (Visualization) を作成します。

5.2. KIBANA を使用したクラスターログの表示

Kibana Web コンソールでクラスターのログを表示します。Kibana でデータを表示し、可視化する方法については、本書では扱いません。詳細は、Kibana ドキュメント を参照してください。

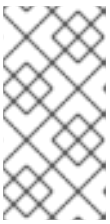
前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。
- Kibana インデックスパターンが存在する。
- Kibana で **infra** および **audit** インデックスを表示するには、ユーザーには **cluster-admin** ロール、 **cluster-reader** ロール、または両方のロールが必要です。デフォルトの **kubeadmin** ユーザーには、これらのインデックスを表示するための適切なパーミッションがあります。**default**、**kube-** および **openshift-** プロジェクトで Pod およびログを表示できる場合、これらのインデックスにアクセスできるはずです。以下のコマンドを使用して、現在のユーザーが適切なパーミッションを持っているかどうかを確認することができます。

```
$ oc auth can-i get pods/log -n <project>
```

出力例

```
yes
```



注記

監査ログは、デフォルトでは内部 OpenShift Container Platform Elasticsearch インスタンスに保存されません。Kibana で監査ログを表示するには、ログ転送 API を使用して監査ログの **default** 出力を使用するパイプラインを設定する必要があります。

手順

Kibana でログを表示するには、以下を実行します。

1. OpenShift Container Platform コンソールで、Application Launcher  をクリックし、**Logging** を選択します。

2. OpenShift Container Platform コンソールにログインするために使用するものと同じ認証情報を使用してログインします。
Kibana インターフェイスが起動します。

3. Kibana で **Discover** をクリックします。

4. 左上隅のドロップダウンメニューから作成したインデックスパターン (**app**、**audit**、または **infra**) を選択します。
ログデータは、タイムスタンプ付きのドキュメントとして表示されます。

5. タイムスタンプ付きのドキュメントの1つを展開します。

6. **JSON** タブをクリックし、ドキュメントのログエントリーを表示します。

例5.1 Kibana のインフラストラクチャーログエントリーのサンプル


```
{
  "_index": "infra-000001",
  "_type": "_doc",
  "_id": "YmJmYTBlNDkZTRmLTliMGQtMjE3NmFiOGUyOWM3",
  "_version": 1,
  "_score": null,
  "_source": {
    "docker": {
      "container_id": "f85fa55bbef7bb783f041066be1e7c267a6b88c4603dfce213e32c1"
    },
    "kubernetes": {
      "container_name": "registry-server",
      "namespace_name": "openshift-marketplace",
      "pod_name": "redhat-marketplace-n64gc",
      "container_image": "registry.redhat.io/redhat/redhat-marketplace-index:v4.6",
      "container_image_id": "registry.redhat.io/redhat/redhat-marketplace-
index@sha256:65fc0c45aabb95809e376feb065771ecda9e5e59cc8b3024c4545c168f",
      "pod_id": "8f594ea2-c866-4b5c-a1c8-a50756704b2a",
      "host": "ip-10-0-182-28.us-east-2.compute.internal",
      "master_url": "https://kubernetes.default.svc",
      "namespace_id": "3abab127-7669-4eb3-b9ef-44c04ad68d38",
      "namespace_labels": {
        "openshift_io/cluster-monitoring": "true"
      },
      "flat_labels": [
        "catalogsource_operators_coreos_com/update=redhat-marketplace"
      ]
    },
    "message": "time=\"2020-09-23T20:47:03Z\" level=info msg=\"serving registry\"
database=/database/index.db port=50051",
    "level": "unknown",
    "hostname": "ip-10-0-182-28.internal",
    "pipeline_metadata": {
      "collector": {
```

```
        "ipaddr4": "10.0.182.28",
        "inputname": "fluent-plugin-systemd",
        "name": "fluentd",
        "received_at": "2020-09-23T20:47:15.007583+00:00",
        "version": "1.7.4 1.6.0"
      }
    },
    "@timestamp": "2020-09-23T20:47:03.422465+00:00",
    "viaq_msg_id": "YmJmYTBlNDktMDMGQtMjE3NmFiOGUyOWM3",
    "openshift": {
      "labels": {
        "logging": "infra"
      }
    }
  },
  "fields": {
    "@timestamp": [
      "2020-09-23T20:47:03.422Z"
    ],
    "pipeline_metadata.collector.received_at": [
      "2020-09-23T20:47:15.007Z"
    ]
  },
  "sort": [
    1600894023422
  ]
}
```

第6章 ログのサードパーティーシステムへの転送

デフォルトで、OpenShift Container Platform クラスターロギングは **ClusterLogging** カスタムリソース (CR) に定義されるデフォルトの内部 Elasticsearch ログストアにログを送信します。

以下の方法を使用して、クラスターロギングを、ログをデフォルトの Elasticsearch ログストアの代わりに OpenShift Container Platform クラスター外の宛先に送信するように設定できます。

- **Fluentd 転送プロトコルを使用したログの送信**。Configmap を使用して Fluentd **転送**プロトコル を使用し、Fluent **転送** プロトコルを受け入れる外部ロギングアグリゲーターにログを安全に送信できます。
- **syslog を使用したログの送信**。設定マップを作成して、syslog プロトコル を使用してログを外部 syslog (RFC 3164) サーバーに送信できます。

または、現在テクノロジープレビューとして ログ転送 API を使用できます。Fluentd プロトコルおよび syslog よりも設定が簡単なログ転送 API は、ログを内部 Elasticsearch ログストアおよび外部の Fluentd ログ集計ソリューションに送信するための設定を公開します。

同じクラスターで設定マップのメソッドおよびログ転送 API を使用することはできません。

重要

ログ転送 API はテクノロジープレビュー機能としてのみご利用いただけます。テクノロジープレビュー機能は Red Hat の実稼働環境でのサービスレベルアグリーメント (SLA) ではサポートされていないため、Red Hat では実稼働環境での使用を推奨していません。Red Hat は実稼働環境でこれらを使用することを推奨していません。テクノロジープレビューの機能は、最新の製品機能をいち早く提供して、開発段階で機能のテストを行いフィードバックを提供していただくことを目的としています。

Red Hat のテクノロジープレビュー機能のサポート範囲についての詳細は、https://access.redhat.com/ja/support/offerings/techpreview/ を参照してください。

設定マップを使用してログを転送する方法は非推奨となり、今後のリリースではログ転送 API に置き換えられます。

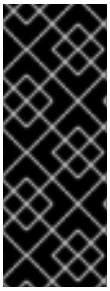
6.1. FLUENTD 転送プロトコルを使用したログの転送

Fluentd **転送** プロトコルを使用して、デフォルトの Elasticsearch ログストアではなく外部のログアグリゲーターにログのコピーを送信できます。OpenShift Container Platform クラスターでは、Fluentd **転送** プロトコルを使用して、このプロトコルを受け入れるように設定されたサーバーにログを送信します。外部ログアグリゲーターを OpenShift Container Platform からログを受信するように設定する必要があります。

注記

ログ転送のこの方法は OpenShift Container Platform では非推奨となり、今後のリリースではログ転送 API に置き換えられます。

Fluentd **転送** プロトコルを使用して OpenShift Container Platform をログを送信するように設定するには、外部ログアグリゲーターを参照する **openshift-logging** namespace の **secure-forward** という ConfigMap を作成します。



重要

OpenShift Container Platform 4.3 以降では、Fluentd **転送** プロトコルを使用するプロセスは変更されています。以下で説明されているように ConfigMap を作成する必要があります。

さらに、設定で必要になる証明書を、Fluentd Pod にマウントされる **secure-forward** という名前のシークレットに追加できます。

secure-forward.conf のサンプル

```
<store>
  @type forward
  <security>
    self_hostname ${hostname} # ${hostname} is a placeholder.
    shared_key "fluent-receiver"
  </security>
  transport tls
  tls_verify_hostname false           # Set false to ignore server cert hostname.

  tls_cert_path '/etc/ocp-forward/ca-bundle.crt'
  <buffer>
    @type file
    path '/var/lib/fluentd/secureforwardlegacy'
    queued_chunks_limit_size "#{ENV['BUFFER_QUEUE_LIMIT'] || '1024' }"
    chunk_limit_size "#{ENV['BUFFER_SIZE_LIMIT'] || '1m' }"
    flush_interval "#{ENV['FORWARD_FLUSH_INTERVAL'] || '5s'}"
    flush_at_shutdown "#{ENV['FLUSH_AT_SHUTDOWN'] || 'false'}"
    flush_thread_count "#{ENV['FLUSH_THREAD_COUNT'] || 2}"
    retry_max_interval "#{ENV['FORWARD_RETRY_WAIT'] || '300'}"
    retry_forever true
    # the systemd journald 0.0.8 input plugin will just throw away records if the buffer
    # queue limit is hit - 'block' will halt further reads and keep retrying to flush the
    # buffer to the remote - default is 'exception' because in_tail handles that case
    overflow_action "#{ENV['BUFFER_QUEUE_FULL_ACTION'] || 'exception'}"
  </buffer>
  <server>
    host fluent-receiver.openshift-logging.svc  # or IP
    port 24224
  </server>
</store>
```

設定に基づく secure-forward ConfigMap のサンプル

```
apiVersion: v1
data:
 secure-forward.conf: "<store>
    \ @type forward
    \ <security>
    \   self_hostname ${hostname} # ${hostname} is a placeholder.
    \   shared_key \"fluent-receiver\"
    \ </security>
    \ transport tls
    \ tls_verify_hostname false           # Set false to ignore server cert hostname.
    \ tls_cert_path '/etc/ocp-forward/ca-bundle.crt'
```

```
    \ <buffer>
    \   @type file
    \   path '/var/lib/fluentd/secureforwardlegacy'
    \   queued_chunks_limit_size \"#{ENV['BUFFER_QUEUE_LIMIT'] || '1024' }\"
    \   chunk_limit_size \"#{ENV['BUFFER_SIZE_LIMIT'] || '1m' }\"
    \   flush_interval \"#{ENV['FORWARD_FLUSH_INTERVAL'] || '5s'}\"
    \   flush_at_shutdown \"#{ENV['FLUSH_AT_SHUTDOWN'] || 'false'}\"
    \   flush_thread_count \"#{ENV['FLUSH_THREAD_COUNT'] || 2}\"
    \   retry_max_interval \"#{ENV['FORWARD_RETRY_WAIT'] || '300'}\"
    \   retry_forever true
    \   # the systemd journald 0.0.8 input plugin will just throw away records if the buffer
    \   # queue limit is hit - 'block' will halt further reads and keep retrying to flush the
    \   # buffer to the remote - default is 'exception' because in_tail handles that case
    \   overflow_action \"#{ENV['BUFFER_QUEUE_FULL_ACTION'] || 'exception'}\"
    \ </buffer>
    \ <server>
    \   host fluent-receiver.openshift-logging.svc  # or IP
    \   port 24224
    \ </server>
    </store>"
kind: ConfigMap
metadata:
  creationTimestamp: "2020-01-15T18:56:04Z"
  name: secure-forward
  namespace: openshift-logging
  resourceVersion: "19148"
  selfLink: /api/v1/namespaces/openshift-logging/configmaps/secure-forward
  uid: 6fd83202-93ab-d851b1d0f3e8
```

手順

OpenShift Container Platform を Fluentd **転送** プロトコルを使用してログを転送できるように設定するには、以下を実行します。

1. **転送** パラメーターについて **secure-forward.conf** という名前の設定ファイルを作成します。

   a. シークレットおよび TLS 情報を設定します。

```
<store>
 @type forward

 self_hostname ${hostname} 1
 shared_key <SECRET_STRING> 2

 transport tls 3

 tls_verify_hostname true 4
 tls_cert_path <path_to_file> 5
```

1 自動生成される証明書の共通名 (CN) のデフォルト値を指定します。

2 ノード間で共有キーを入力します。

3 **tls** を指定して TLS 検証を有効にします。

4 サーバー証明書のホスト名を確認するには **true** に設定します。サーバー証明書のホス

ト名を無視するには、**false** に設定します。

5 プライベート CA 証明書ファイルへのパスを **/etc/ocp-forward/ca_cert.pem** として指定します。

mTLS を使用するには、クライアント証明書およびキーパラメーターなどの設定に関する情報として Fluentd のドキュメント を参照してください。

b. 外部 Fluentd サーバーの名前、ホスト、およびポートを設定します。

```
<server>
  name 1
  host 2
  hostlabel 3
  port 4
</server>
<server> 5
  name
  host
</server>
```

1 オプションで、このサーバーの名前を入力します。

2 サーバーのホスト名または IP を指定します。

3 サーバーのホストラベルを指定します。

4 サーバーのポートを指定します。

5 オプションで、サーバーを追加します。2 つ以上のサーバーを指定する場合、**forward** はこれらのサーバーノードをラウンドロビン順で使用します。

以下は例になります。

```
<server>
  name externalserver1
  host 192.168.1.1
  hostlabel externalserver1.example.com
  port 24224
</server>
<server>
  name externalserver2
  host externalserver2.example.com
  port 24224
</server>
</store>
```

2. 設定ファイルから **openshift-logging** namespace に **secure-forward** という名前の ConfigMap を作成します。

```
$ oc create configmap secure-forward --from-file=secure-forward.conf -n openshift-logging
```

3. オプション: レシーバーに必要なシークレットをインポートします。

```
$ oc create secret generic secure-forward --from-file=<arbitrary-name-of-
key1>=cert_file_from_fluentd_receiver --from-
literal=shared_key=value_from_fluentd_receiver
```

以下は例になります。

```
$ oc create secret generic secure-forward --from-file=ca-bundle.crt=ca-for-fluentd-
receiver/ca.crt --from-literal=shared_key=fluentd-receiver
```

4. **fluentd** Pod を更新し、**secure-forward** シークレットおよび **secure-forward** ConfigMap を適用します。

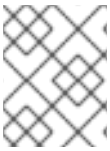
```
$ oc delete pod --selector logging-infra=fluentd
```

5. 外部ログアグリゲーターを OpenShift Container Platform からメッセージを安全に受信できるように設定します。

6.2. SYSLOG プロトコルを使用したログの転送

syslog プロトコルを使用して、デフォルトの Elasticsearch ログストアではなく外部の syslog サーバーにログのコピーを送信できます。この **syslog** プロトコルについては、以下の点に注意してください。

- RFC 5424 ではなく、syslog プロトコル (RFC 3164) を使用する
- TLS に対応していないため、安全ではない
- Kubernetes メタデータ、systemd データその他のメタデータを提供しない



注記

ログ転送のこの方法は OpenShift Container Platform では非推奨となり、今後のリリースではログ転送 API に置き換えられます。

syslog プロトコルには、以下の 2 つのバージョンがあります。

- **out_syslog**: UDP で通信するバッファーなしの実装は、データをバッファーせずに結果を即時に書き込みます。
- **out_syslog_buffered**: TCP で通信するバッファーの実装は、データをいくつかのチャンクにバッファーリングします。

syslog プロトコルを使用してログ転送を設定するには、ログを転送するために必要な情報を使って **syslog.conf** という設定ファイルを作成します。次に、そのファイルを使用して OpenShift Container Platform がログの転送時に使用する **openshift-logging** namespace の **syslog** という ConfigMap を作成します。syslog サーバーを OpenShift Container Platform からログを受信するように設定する必要があります。

重要

OpenShift Container Platform 4.3 以降では、**syslog** プロトコルを使用するプロセスは変更されています。以下で説明されているように ConfigMap を作成する必要があります。

設定ファイルに別個の **<store>** スタンザを指定して、ログを複数の syslog サーバーに転送できます。

サンプル syslog.conf

```
<store>
@type syslog_buffered (1)
remote_syslog rsyslogserver.openshift-logging.svc.cluster.local (2)
port 514 (3)
hostname ${hostname} (4)
remove_tag_prefix tag (5)
tag_key ident,systemd.u.SYSLOG_IDENTIFIER (6)
facility local0 (7)
severity info (8)
use_record true (9)
payload_key message (10)
</store>
```

(1) **syslog** プロトコル (**syslog** または **syslog_buffered** のいずれか)。

(2) syslog サーバーの完全修飾ドメイン名 (FQDN) または IP アドレス。

(3) 接続先のポート番号。デフォルトは **514** です。

(4) syslog サーバーの名前。

(5) タグから接頭辞を削除します。デフォルトは **''** (空) です。

(6) syslog キーを設定するためのフィールド。

(7) syslog ログファシリティーまたはソース。

(8) syslog ログの重大度。

(9) レコードの重大度とファシリティーを使用するかどうかを決定する (ある場合)。

(10) オプション。syslog メッセージのペイロードを設定するためのキー。デフォルトは **message** に設定されます。

注記

payload_key パラメーターを設定すると、他のパラメーターが syslog に転送されなくなります。

サンプル syslog.conf をベースとするサンプル syslog ConfigMap

```
kind: ConfigMap
apiVersion: v1
metadata:
  name: syslog
  namespace: openshift-logging
data:
  syslog.conf: |
    <store>
     @type syslog_buffered
```

```
remote_syslog syslogserver.openshift-logging.svc.cluster.local
port 514
hostname ${hostname}
remove_tag_prefix tag
tag_key ident,systemd.u.SYSLOG_IDENTIFIER
facility local0
severity info
use_record true
payload_key message
</store>
```

手順

OpenShift Container Platform が **syslog** プロトコルを使用してログを転送するように設定するには、以下を実行します。

1. **<store>** スタンザ内に以下のパラメーターが含まれる **syslog.conf** という名前の設定ファイルを作成します。

   a. **syslog** プロトコルタイプを指定します。

   ```
   @type syslog_buffered 1
   ```

   1 使用するプロトコル (**syslog** または **syslog_buffered** のいずれか) を指定します。

   b. 外部 syslog サーバーの名前、ホスト、およびポートを設定します。

   ```
   remote_syslog <remote> 1
   port <number> 2
   hostname <name> 3
   ```

   1 syslog サーバーの FQDN または IP アドレスを指定します。

   2 syslog サーバーのポートを指定します。

   3 この syslog サーバーの名前を指定します。

   以下は例になります。

   出力例

   ```
   remote_syslog syslogserver.openshift-logging.svc.cluster.local
   port 514
   hostname fluentd-server
   ```

   c. 必要に応じて他の syslog 変数を設定します。

   ```
   remove_tag_prefix 1
   tag_key <key> 2
   facility <value> 3
   ```

```
severity <value> 4
use_record <value> 5
payload_key message 6
```

1. このパラメーターを追加して、**tag** フィールドを syslog 接頭辞から削除します。
2. syslog キーを設定するためのフィールドを指定します。
3. syslog ログファシリティーまたはソースを指定します。値については、RTF 3164 を参照してください。
4. syslog ログの重大度を指定します。値については、RTF 3164 リンクを参照してください。
5. **true** を指定して、レコードの重大度およびファシリティーを使用します (ある場合)。**true** の場合、**container_name**、**namespace_name**、および **pod_name** は、出力の内容に組み込まれます。
6. syslog メッセージのペイロードを設定するためにキーを指定します。デフォルトは **message** に設定されます。

出力例

```
facility local0
severity info
```

設定ファイルは以下のように表示されます。

```
<store>
@type syslog_buffered
remote_syslog syslogserver.openshift-logging.svc.cluster.local
port 514
hostname ${hostname}
tag_key ident,systemd.u.SYSLOG_IDENTIFIER
facility local0
severity info
use_record false
</store>
```

2. 設定ファイルから **openshift-logging** namespace に **syslog** という名前の ConfigMap を作成します。

```
$ oc create configmap syslog --from-file=syslog.conf -n openshift-logging
```

Cluster Logging Operator は Fluentd Pod を再デプロイします。Pod が再デプロイされない場合、強制的に再デプロイするために Fluentd Pod を削除できます。

```
$ oc delete pod --selector logging-infra=fluentd
```

6.3. ログ転送 API を使用したログの転送

ログ転送 API により、コンテナーおよびノードログをクラスター内外の特定のエンドポイントに送信で

きるようにカスタムパイプラインを設定できます。既存のロギングサービス、外部 Elasticsearch クラスター、外部ログ集計ソリューション、またはセキュリティー情報およびイベント管理 (SIEM) システムなどの OpenShift Container Platform クラスターロギングで管理されていないリモート宛先および内部 OpenShift Container Platform Elasticsearch インスタンスにログをタイプ別に送信することができます。

重要

ログ転送 API は現時点ではテクノロジープレビュー機能です。テクノロジープレビュー機能は、Red Hat の実稼働環境でのサービスレベルアグリーメント (SLA) ではサポートされていないため、Red Hat では実稼働環境での使用を推奨していません。これらの機能は、近々発表予定の製品機能をリリースに先駆けてご提供することにより、お客様は機能性をテストし、開発プロセス中にフィードバックをお寄せいただくことができます。

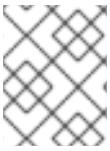
詳細は、テクノロジープレビュー機能のサポート範囲 を参照してください。

異なるタイプのログを異なるシステムに送信して、組織の誰がそれぞれのタイプにアクセスできるかを制御できます。オプションの TLS サポートにより、組織の必要に応じてセキュアな通信を使用してログを送信することができます。

ログ転送 API の使用はオプションです。ログを内部の OpenShift Container Platform Elasticsearch インスタンスのみに転送する必要がある場合は、ログ転送 API を設定しないようにしてください。

6.3.1. ログ転送 API について

ログ転送 API を使用してクラスターログを転送するには、**出力** と **パイプライン** の組み合わせが必要です。これらのリソースは、OpenShift Container Platform クラスター内外の特定のエンドポイントにログを送信します。



注記

デフォルトの内部 OpenShift Container Platform Elasticsearch ログストアのみを使用する必要がある場合は、出力およびパイプラインは設定しません。

output はログデータの宛先で、パイプラインは単一のソースまたは 1 つまたは複数の出力の単純なルーティングを定義します。

出力には、以下のいずれかが該当します。

- **elasticsearch** を使用して、サーバー名または FQDN、および/または内部 OpenShift Container Platform Elasticsearch ログストアで指定される、外部の Elasticsearch 6 (すべてのリリース)クラスターにログを転送します。
- **forward** を使用して、ログを外部のログ集計ソリューションに転送します。このオプションは Fluentd **forward** プロトコルを使用します。

パイプライン は、データの種類を出力に関連付けます。転送できるデータのタイプは以下のいずれかになります。

- **logs.app**: クラスターで実行される、インフラストラクチャーコンテナーアプリケーションを除くユーザーアプリケーションによって生成されるコンテナーログ。
- **logs.infra**: ジャーナルログなどの、クラスターで実行されるインフラストラクチャーコンポーネントおよび OpenShift Container Platform ノードの両方で生成されるログ。インフラストラ

クチャーコンポーネントは、**openshift***、 **kube***、または **default** プロジェクトで実行される Pod です。

- **logs.audit**: ノード監査システム (auditd) で生成されるログ (**/var/log/audit/audit.log** ファイルに保存される)、および Kubernetes apiserver および OpenShift apiserver の監査ログ。

ログ転送 API を使用するには、出力およびパイプラインと共にカスタム **logforwarding** 設定ファイルを作成し、指定した宛先にログを送信します。

以下の点に注意してください。

- 内部 OpenShift Container Platform Elasticsearch ログストアは、監査ログのセキュアなストレージを提供しません。監査ログを転送するシステムが組織および政府の規制に準拠しており、適切にセキュリティーが保護されていることを確認することが推奨されています。OpenShift Container Platform クラスターロギングはこれらの規制に準拠しません。

- 出力は、シークレットを使用する TLS 通信をサポートします。シークレットには、**tls.crt**、**tls.key**、および **ca-bundle.crt** のキーが含まれる必要があります。これらは、それぞれが表す証明書を参照します。転送機能を安全な方法で使用するには、シークレットにキー **shared_key** が含まれる必要があります。

- キーやシークレット、サービスアカウント、ポートのオープン、またはグローバルプロキシー設定など、外部の宛先で必要となる可能性のある追加設定を作成し、維持する必要があります。

以下の例は、3 つの出力を作成します。

- 内部 OpenShift Container Platform Elasticsearch ログストア

- 非セキュアな外部で管理される Elasticsearch ログストア

- セキュアな外部ログアグリゲーター (**forward** プロトコルを使用)。

3 つのパイプラインは以下を送信します。

- 内部 OpenShift Container Platform Elasticsearch ログストアへのアプリケーションログ

- 外部 Elasticsearch ログストアへのインフラストラクチャーログ

- セキュリティーが保護されたデバイスへの監査ログ (**forward** プロトコルを使用)

ログ転送の出力とパイプラインのサンプル

```
apiVersion: "logging.openshift.io/v1alpha1"
kind: "LogForwarding"
metadata:
  name: instance (1)
  namespace: openshift-logging
spec:
  disableDefaultForwarding: true (2)
  outputs: (3)
   - name: elasticsearch (4)
     type: "elasticsearch" (5)
     endpoint: elasticsearch.openshift-logging.svc:9200 (6)
     secret: (7)
       name: fluentd
```

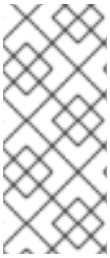
```
  - name: elasticsearch-insecure
    type: "elasticsearch"
    endpoint: elasticsearch-insecure.messaging.svc.cluster.local
    insecure: true 8
  - name: secureforward-offcluster
    type: "forward"
    endpoint: https://secureforward.offcluster.com:24224
    secret:
      name: secureforward
pipelines: 9
  - name: container-logs 10
    inputSource: logs.app 11
    outputRefs: 12
    - elasticsearch
    - secureforward-offcluster
  - name: infra-logs
    inputSource: logs.infra
    outputRefs:
    - elasticsearch-insecure
  - name: audit-logs
    inputSource: logs.audit
    outputRefs:
    - secureforward-offcluster
```

1. ログ転送 CR の名前は **instance** である必要があります。
2. ログ転送を有効にするパラメーター。ログ転送を有効にするには **true** に設定します。
3. 出力の設定。
4. 出力を記述する名前。
5. **elasticsearch** または **forward** のいずれかの出力タイプ。
6. ログ転送エンドポイント (サーバー名または FQDN のいずれか)。内部 OpenShift Container Platform Elasticsearch ログストアの場合は、**elasticsearch.openshift-logging.svc:9200** を指定します。
7. TLS 通信のエンドポイントで必要なシークレットのオプションの名前。シークレットは **openshift-logging** プロジェクトに存在する必要があります。
8. エンドポイントがシークレットを使用しない場合のオプションの設定 (これにより、非セキュアな通信が発生します)。
9. パイプラインの設定。
10. パイプラインを説明する名前。
11. ソースタイプ (**logs.app**、**logs.infra**、または **logs.audit**)。
12. CR に設定される単一または複数の出力の名前。

外部ログアグリゲーターが利用できない場合の Fluentd のログの処理

外部ロギングアグリゲーターが利用できず、ログを受信できない場合、Fluentd は継続してログを収集し、それらをバッファーに保存します。ログアグリゲーターが利用可能になると、バッファーされたロ

グを含む、ログの転送が再開されます。バッファーが完全に一杯になると、Fluentd はログの収集を停止します。OpenShift Container Platform はログをローテーションし、それらを削除します。バッファーサイズを調整したり、永続ボリューム要求 (PVC) を Fluentd デーモンセットまたは Pod に追加したりすることはできません。



注記

内部 OpenShift Container Platform Elasticsearch ログストアは監査ログのセキュアなストレージを提供しないため、デフォルトで監査ログは内部 Elasticsearch インスタンスに保存されません。監査ログを内部ログストアに送信する必要がある場合 (Kibana で監査ログを表示するなど)、Forward audit logs to the log store で説明されているようにログ転送 API を使用する必要があります。

6.3.2. ログ転送 API の有効化

API を使用してログを転送する前に、ログ転送 API を有効にする必要があります。

手順

ログ転送 API を有効にするには、以下を実行します。

1. **openshift-logging** プロジェクトで **ClusterLogging** カスタムリソース (CR) を編集します。

```
$ oc edit ClusterLogging instance
```

2. **clusterlogging.openshift.io/logforwardingtechpreview** アノテーションを追加し、**enabled** に設定します。

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  annotations:
    clusterlogging.openshift.io/logforwardingtechpreview: enabled (1)
  name: "instance"
  namespace: "openshift-logging"
spec:

...

  collection: (2)
    logs:
      type: "fluentd"
      fluentd: {}
```

(1) ログ転送 API を有効および無効にします。ログ転送を使用するには、**enabled** に設定します。OpenShift Container Platform Elasticsearch インスタンスのみを使用するには、disable に設定するか、またはアノテーションを追加しません。

(2) Fluentd を使用できるように、**spec.collection** ブロックを **ClusterLogging** CR で定義する必要があります。

6.3.3. ログ転送 API を使用したログ転送の設定

ログ転送を設定するには、クラスターロギングの **ClusterLogging** (CR) を編集し

て、**clusterlogging.openshift.io/logforwardingtechpreview: enabled** アノテーションを追加し、**LogForwarding** カスタムリソースを作成して出力、パイプラインを指定し、ログ転送を有効にします。

ログ転送を有効にする場合、次の 3 つのソースタイプのすべてのパイプラインを定義する必要があります (**logs.app**、**logs.infra**、および **logs.audit**)。未定義のソースタイプのログはすべてドロップされます。たとえば、**logs.app** および **log-audit** タイプのパイプラインを指定するものの、**logs.infra** タイプのパイプラインを指定していない場合、**logs.infra** ログがドロップされます。

手順

API を使用してログ転送を設定するには、以下を実行します。

1. 以下のような **LogForwarding** CR YAML ファイルを作成します。

```
apiVersion: "logging.openshift.io/v1alpha1"
kind: "LogForwarding"
metadata:
  name: instance (1)
  namespace: openshift-logging (2)
spec:
  disableDefaultForwarding: true (3)
  outputs: (4)
   - name: elasticsearch
     type: "elasticsearch"
     endpoint: elasticsearch.openshift-logging.svc:9200
     secret:
        name: fluentd
   - name: elasticsearch-insecure
     type: "elasticsearch"
     endpoint: elasticsearch-insecure.messaging.svc.cluster.local
     insecure: true
   - name: secureforward-offcluster
     type: "forward"
     endpoint: https://secureforward.offcluster.com:24224
     secret:
        name: secureforward
  pipelines: (5)
   - name: container-logs
     inputSource: logs.app
     outputRefs:
     - elasticsearch
     - secureforward-offcluster
   - name: infra-logs
     inputSource: logs.infra
     outputRefs:
     - elasticsearch-insecure
   - name: audit-logs
     inputSource: logs.audit
     outputRefs:
     - secureforward-offcluster
```

(1) ログ転送 CR の名前は **instance** である必要があります。

(2) ログ転送 CR の namespace は **openshift-logging** である必要があります。

3 **true** に設定されると、デフォルトのログ転送動作が無効になります。

4 1 つ以上のエンドポイントを追加するには、以下を実行します。

- **elasticsearch** または **forward** のいずれかの出力タイプを指定します。
- 出力の名前を入力します。
- サーバー名、FQDN、または IP アドレスのいずれかのエンドポイントを入力します。CIDR アノテーションを使用するクラスター全体のプロキシーが有効になっている場合、エンドポイントは IP アドレスではなくサーバー名または FQDN である必要があります。内部 OpenShift Container Platform Elasticsearch インスタンスの場合は、**elasticsearch.openshift-logging.svc:9200** を指定します。
- オプション: TLS 通信のエンドポイントに必要なシークレットの名前を入力します。シークレットは **openshift-logging** プロジェクトに存在する必要があります。
- エンドポイントがシークレットを使用しない場合に **insecure: true** を指定します (これにより、非セキュアな通信が発生します)。

5 1 つ以上のパイプラインを追加します。

- パイプラインの名前を入力します。
- ソースタイプ (**logs.app**、**logs.infra**、または **logs.audit**) を指定します。
- CR に設定された 1 つ以上の出力の名前を指定します。

注記

disableDefaultForwarding: true を設定する場合、アプリケーション、インフラストラクチャーおよび監査の 3 つの種類のログすべてのパイプラインおよび出力を設定する必要があります。ログの種類に対応するパイプラインおよび出力を指定しない場合、それらのログは保存されず、失われます。

2. CR オブジェクトを作成します。

```
$ oc create -f <file-name>.yaml
```

6.3.3.1. ログ転送カスタムリソースのサンプル

通常のログ転送設定は以下の例のようになります。

以下のログ転送カスタムリソースは、すべてのログをセキュアな Elasticsearch ログストアに送信します。

Elasticsearch ログストアに転送するカスタムリソースのサンプル

```
apiVersion: logging.openshift.io/v1alpha1
kind: LogForwarding
metadata:
  name: instance
  namespace: openshift-logging
```

```
spec:
  disableDefaultForwarding: true
  outputs:
    - name: user-created-es
      type: elasticsearch
      endpoint: 'elasticsearch-server.openshift-logging.svc:9200'
      secret:
        name: piplinesecret
  pipelines:
    - name: app-pipeline
      inputSource: logs.app
      outputRefs:
        - user-created-es
    - name: infra-pipeline
      inputSource: logs.infra
      outputRefs:
        - user-created-es
    - name: audit-pipeline
      inputSource: logs.audit
      outputRefs:
        - user-created-es
```

以下のログ転送カスタムリソースは、Fluentd **forward** プロトコルを使用してすべてのログをセキュアな Fluentd インスタンスに送信します。

forward プロトコルを使用するためのサンプルカスタムリソース

```
apiVersion: logging.openshift.io/v1alpha1
kind: LogForwarding
metadata:
  name: instance
  namespace: openshift-logging
spec:
  disableDefaultForwarding: true
  outputs:
    - name: fluentd-created-by-user
      type: forward
      endpoint: 'fluentdserver.openshift-logging.svc:24224'
      secret:
        name: fluentdserver
  pipelines:
    - name: app-pipeline
      inputSource: logs.app
      outputRefs:
        - fluentd-created-by-user
    - name: infra-pipeline
      inputSource: logs.infra
      outputRefs:
        - fluentd-created-by-user
    - name: clo-default-audit-pipeline
      inputSource: logs.audit
      outputRefs:
        - fluentd-created-by-user
```

6.3.4. ログ転送 API の無効化

ログ転送 API を無効にし、指定されたエンドポイントへのログの転送を停止するには、**metadata.annotations.clusterlogging.openshift.io/logforwardingtechpreview:enabled** パラメーターを **ClusterLogging** CR から削除してから **LogForwarding** CR を削除します。コンテナーおよびノードログは内部 OpenShift Container Platform Elasticsearch インスタンスに転送されます。

注記

disableDefaultForwarding=false を設定すると、クラスターロギングがログを指定されたエンドポイント **および** デフォルトの内部 OpenShift Container Platform Elasticsearch インスタンスに送信できなくなります。

手順

ログ転送 API を無効にするには、以下を実行します。

1. **openshift-logging** プロジェクトで **ClusterLogging** カスタムリソース (CR) を編集します。

```
$ oc edit ClusterLogging instance
```

2. **clusterlogging.openshift.io/logforwardingtechpreview** アノテーションを削除します。

```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  annotations:
    clusterlogging.openshift.io/logforwardingtechpreview: enabled (1)
  name: "instance"
  namespace: "openshift-logging"
....
```

(1) このアノテーションを削除します。

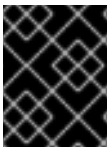
3. ログ転送カスタムリソースを削除します。

```
$ oc delete LogForwarding instance -n openshift-logging
```

第7章 KUBERNETES イベントの収集および保存

OpenShift Container Platform イベントルーターは、Kubernetes イベントを監視し、それらをクラスターロギングによって収集できるようにログに記録する Pod です。イベントルーターは手動でデプロイする必要があります。

イベントルーターはすべてのプロジェクトからイベントを収集し、それらを **STDOUT** に書き込みます。Fluentd はそれらのイベントを収集し、それらを OpenShift Container Platform Elasticsearch インスタンスに転送します。Elasticsearch はイベントを **infra** インデックスにインデックス化します。



重要

イベントルーターは追加の負荷を Fluentd に追加し、処理できる他のログメッセージの数に影響を与える可能性があります。

7.1. イベントルーターのデプロイおよび設定

以下の手順を使用してイベントルーターをクラスターにデプロイします。イベントルーターを **openshift-logging** プロジェクトに常にデプロイし、クラスター全体でイベントが収集されるようにする必要があります。

以下のテンプレートオブジェクトは、イベントルーターに必要なサービスアカウント、クラスターロールおよびクラスターロールバインディングを作成します。テンプレートはイベントルーター Pod も設定し、デプロイします。このテンプレートは変更せずに使用するか、デプロイメントオブジェクトの CPU およびメモリー要求を変更することができます。

前提条件

- サービスアカウントを作成し、クラスターロールバインディングを更新するには、適切なパーミッションが必要です。たとえば、以下のテンプレートを、**cluster-admin** ロールを持つユーザーで実行できます。
- クラスターロギングがインストールされている必要があります。

手順

1. イベントルーターのテンプレートを作成します。

```
kind: Template
apiVersion: v1
metadata:
  name: eventrouter-template
  annotations:
    description: "A pod forwarding kubernetes events to cluster logging stack."
    tags: "events,EFK,logging,cluster-logging"
objects:
  - kind: ServiceAccount (1)
    apiVersion: v1
    metadata:
      name: eventrouter
      namespace: ${NAMESPACE}
  - kind: ClusterRole (2)
    apiVersion: v1
    metadata:
```

```
    name: event-reader
  rules:
  - apiGroups: [""]
    resources: ["events"]
    verbs: ["get", "watch", "list"]
- kind: ClusterRoleBinding (3)
  apiVersion: v1
  metadata:
    name: event-reader-binding
  subjects:
  - kind: ServiceAccount
    name: eventrouter
    namespace: ${NAMESPACE}
  roleRef:
    kind: ClusterRole
    name: event-reader
- kind: ConfigMap (4)
  apiVersion: v1
  metadata:
    name: eventrouter
    namespace: ${NAMESPACE}
  data:
    config.json: |-
      {
        "sink": "stdout"
      }
- kind: Deployment (5)
  apiVersion: apps/v1
  metadata:
    name: eventrouter
    namespace: ${NAMESPACE}
    labels:
      component: eventrouter
      logging-infra: eventrouter
      provider: openshift
  spec:
    selector:
      matchLabels:
        component: eventrouter
        logging-infra: eventrouter
        provider: openshift
    replicas: 1
    template:
      metadata:
        labels:
          component: eventrouter
          logging-infra: eventrouter
          provider: openshift
        name: eventrouter
      spec:
        serviceAccount: eventrouter
        containers:
          - name: kube-eventrouter
            image: ${IMAGE}
            imagePullPolicy: IfNotPresent
            resources:
```

```
            requests:
              cpu: ${CPU}
              memory: ${MEMORY}
            volumeMounts:
            - name: config-volume
              mountPath: /etc/eventrouter
          volumes:
            - name: config-volume
              configMap:
                name: eventrouter
parameters:
  - name: IMAGE
    displayName: Image
    value: "registry.redhat.io/openshift4/ose-logging-eventrouter:latest"
  - name: CPU (6)
    displayName: CPU
    value: "100m"
  - name: MEMORY (7)
    displayName: Memory
    value: "128Mi"
  - name: NAMESPACE
    displayName: Namespace
    value: "openshift-logging" (8)
```

1. イベントルーターの **openshift-logging** プロジェクトでサービスアカウントを作成します。
2. ClusterRole を作成し、クラスター内のイベントを監視します。
3. ClusterRoleBinding を作成し、ClusterRole をサービスアカウントにバインドします。
4. **openshift-logging** プロジェクトで設定マップを作成し、必要な **config.json** ファイルを生成します。
5. **openshift-logging** プロジェクトでデプロイメントを作成し、イベントルーター Pod を生成し、設定します。
6. イベントルーター Pod に割り当てるメモリーの最小量を指定します。デフォルトは **128Mi** に設定されます。
7. イベントルーター Pod に割り当てる CPU の最小量を指定します。デフォルトは **100m** に設定されます。
8. オブジェクトをインストールする **openshift-logging** プロジェクトを指定します。

2. 以下のコマンドを使用してテンプレートを処理し、これを適用します。

```
$ oc process -f <templatefile> | oc apply -n openshift-logging -f -
```

以下に例を示します。

```
$ oc process -f eventrouter.yaml | oc apply -n openshift-logging -f -
```

出力例

```
serviceaccount/logging-eventrouter created
clusterrole.authorization.openshift.io/event-reader created
clusterrolebinding.authorization.openshift.io/event-reader-binding created
configmap/logging-eventrouter created
deployment.apps/logging-eventrouter created
```

3. イベントルーターが **openshift-logging** プロジェクトにインストールされていることを確認します。

   a. 新規イベントルーター Pod を表示します。

   ```
   $ oc get pods --selector  component=eventrouter -o name -n openshift-logging
   ```

   出力例

   ```
   pod/cluster-logging-eventrouter-d649f97c8-qvv8r
   ```

   b. イベントルーターによって収集されるイベントを表示します。

   ```
   $ oc logs <cluster_logging_eventrouter_pod> -n openshift-logging
   ```

   以下に例を示します。

   ```
   $ oc logs cluster-logging-eventrouter-d649f97c8-qvv8r -n openshift-logging
   ```

   出力例

   ```
   {"verb":"ADDED","event":{"metadata":{"name":"openshift-service-catalog-controller-manager-remover.1632d931e88fcd8f","namespace":"openshift-service-catalog-removed","selfLink":"/api/v1/namespaces/openshift-service-catalog-removed/events/openshift-service-catalog-controller-manager-remover.1632d931e88fcd8f","uid":"787d7b26-3d2f-4017-b0b0-420db4ae62c0","resourceVersion":"21399","creationTimestamp":"2020-09-08T15:40:26Z"},"involvedObject":{"kind":"Job","namespace":"openshift-service-catalog-removed","name":"openshift-service-catalog-controller-manager-remover","uid":"fac9f479-4ad5-4a57-8adc-cb25d3d9cf8f","apiVersion":"batch/v1","resourceVersion":"21280"},"reason":"Completed","message":"Job completed","source":{"component":"job-controller"},"firstTimestamp":"2020-09-08T15:40:26Z","lastTimestamp":"2020-09-08T15:40:26Z","count":1,"type":"Normal"}}
   ```

   また、Elasticsearch **infra** インデックスを使用してインデックスパターンを作成し、Kibana を使用してイベントを表示することもできます。

第8章 クラスターロギングの更新

OpenShift Container Platform クラスターを 4.4 から 4.5 に更新した後に、Elasticsearch Operator および Cluster Logging Operator を 4.4 から 4.5 に更新できます。

クラスターロギング 4.5 では、新規 Elasticsearch バージョン Elasticsearch 6.8.1 および Elasticsearch の強化されたセキュリティープラグイン Open Distro が導入されています。新規 Elasticsearch バージョンでは、新規 Elasticsearch データモデルが導入されました。この場合、Elasticsearch データはタイプ (インフラストラクチャー、アプリケーション、および監査) でのみインデックス化されます。以前のバージョンでは、データはタイプ (インフラストラクチャーおよびアプリケーション) およびプロジェクトでインデックス化されていました。

重要

新規データモデルにより、更新により、既存のカスタム Kibana インデックスパターンおよびビジュアライゼーションは新規バージョンに移行しません。更新後、Kibana インデックスパターンおよびビジュアライゼーションを、新規インデックスに一致させるように再作成する必要があります。

これらの変更の性質上、クラスターロギングを 4.5 に更新する必要はありません。ただし、OpenShift Container Platform 4.6 に更新する場合は、その時点でクラスターロギングを 4.6 に更新する必要があります。

8.1. クラスターロギングの更新

OpenShift Container Platform クラスターの更新後に、Elasticsearch Operator および Cluster Logging Operator のサブスクリプションを変更して、クラスターロギングを 4.4 から 4.5 に更新できます。

更新時に以下を行います。

- Cluster Logging Operator を更新する前に Elasticsearch Operator を更新する必要があります。
- Elasticsearch Operator と Cluster Logging Operator の両方を更新する必要があります。Elasticsearch Operator が更新されても、Cluster Logging Operator が更新されない場合、Kibana は使用できなくなります。

  Elasticsearch Operator の前に Cluster Logging Operator を更新する場合、Kibana は更新されず、Kibana カスタムリソース (CR) は作成されません。この問題を回避するには、Cluster Logging Operator Pod を削除します。Cluster Logging Operator Pod が再デプロイされると、Kibana CR が作成されます。

重要

クラスターロギングのバージョンが 4.4 よりも前の場合、クラスターロギングを 4.5 に更新する前に 4.4 にアップグレードする必要があります。

前提条件

- OpenShift Container Platform クラスターを 4.4 から 4.5 に更新します。
- クラスターロギングのステータスが正常であることを確認します。
  - すべての Pod が **Ready** 状態にある。

- Elasticsearch クラスターが正常である。

- Elasticsearch および Kibana データをバックアップします。

- 内部 Elasticsearch インスタンスが永続ボリューム要求 (PVC) を使用する場合、PVC には **logging-cluster:elasticsearch** ラベルが含まれる必要があります。ラベルがない場合、アップグレード時にガベージコレクションプロセスではそれらの PVC が削除され、Elasticsearch Operator は新規 PVC を作成します。

  - バージョン 4.4.30 より前の OpenShift Container Platform バージョンから更新する場合は、ラベルを Elasticsearch PVC に手動で追加する必要があります。
    たとえば、以下のコマンドを使用してラベルをすべての Elasticsearch PVC に追加できます。

    ```
    $ oc label pvc --all -n openshift-logging logging-cluster=elasticsearch
    ```

  - OpenShift Container Platform 4.4.30 以降では、Elasticsearch Operator はラベルを PVC に自動的に追加します。

手順

1. Elasticsearch Operator を更新します。

   a. Web コンソールで **Operators → Installed Operators** をクリックします。

   b. **openshift-operators-redhat** プロジェクトを選択します。

   c. **Elasticsearch Operator**をクリックします。

   d. **Subscription → Channel** をクリックします。

   e. **Change Subscription Update Channel**ウィンドウで **4.5** を選択し、**Save** をクリックします。

   f. 数秒待ってから **Operators → Installed Operators** をクリックします。
   Elasticsearch Operator が 4.5 と表示されます。以下は例になります。

   ```
   Elasticsearch Operator
   4.5.0-202007012112.p0 provided
   by Red Hat, Inc
   ```

   Status フィールドで **Succeeded** を報告するのを待機します。

2. Cluster Logging Operator を更新します。

   a. Web コンソールで **Operators → Installed Operators** をクリックします。

   b. **openshift-logging** プロジェクトを選択します。

   c. **Cluster Logging Operator**をクリックします。

   d. **Subscription → Channel** をクリックします。

   e. **Change Subscription Update Channel**ウィンドウで **4.5** を選択し、**Save** をクリックします。

f. 数秒待ってから **Operators → Installed Operators** をクリックします。
Cluster Logging Operator は 4.5 として表示されます。以下は例になります。

```
Cluster Logging
4.5.0-202007012112.p0 provided
by Red Hat, Inc
```

Status フィールドで **Succeeded** を報告するのを待機します。

3. ロギングコンポーネントを確認します。

a. すべての Elasticsearch Pod が **Ready** ステータスであることを確認します。

```
$ oc get pod -n openshift-logging --selector component=elasticsearch
```

出力例

```
NAME                                            READY   STATUS    RESTARTS   AGE
elasticsearch-cdm-1pbrl44l-1-55b7546f4c-mshhk   2/2     Running   0          31m
elasticsearch-cdm-1pbrl44l-2-5c6d87589f-gx5hk   2/2     Running   0          30m
elasticsearch-cdm-1pbrl44l-3-88df5d47-m45jc     2/2     Running   0          29m
```

b. Elasticsearch クラスターが正常であることを確認します。

```
$ oc exec -n openshift-logging -c elasticsearch elasticsearch-cdm-1pbrl44l-1-
55b7546f4c-mshhk -- es_cluster_health
```

```
{
  "cluster_name" : "elasticsearch",
  "status" : "green",
}
...
```

c. Elasticsearch cron ジョブが作成されていることを確認します。

```
$ oc project openshift-logging
```

```
$ oc get cronjob
```

```
NAME                     SCHEDULE       SUSPEND   ACTIVE   LAST SCHEDULE   AGE
elasticsearch-im-app     */15 * * * *   False     0        <none>          56s
elasticsearch-im-audit   */15 * * * *   False     0        <none>          56s
elasticsearch-im-infra   */15 * * * *   False     0        <none>          56s
```

d. ログストアが 4.5 に更新され、インデックスが **green** であることを確認します。

```
$ oc exec -c elasticsearch <any_es_pod_in_the_cluster> -- indices
```

出力に **app-00000x**、 **infra-00000x**、**audit-00000x**、**.security** インデックス が含まれることを確認します。

例8.1 緑色のステータスのインデックスを含む出力例

```
Tue Jun 30 14:30:54 UTC 2020
health status index                                                    uuid                   pri rep
docs.count docs.deleted store.size pri.store.size
green  open   infra-000008
bnBvUFEXTWi92z3zWAzieQ   3 1      222195            0       289          144
green  open   infra-000004
rtDSzoqsSl6saisSK7Au1Q   3 1      226717            0       297          148
green  open   infra-000012
RSf_kUwDSR2xEuKRZMPqZQ   3 1      227623            0       295          147
green  open   .kibana_7
1SJdCqlZTPWlIAaOUd78yg   1 1          4            0         0            0
green  open   infra-000010
iXwL3bnqTuGEABbUDa6OVw   3 1      248368            0       317          158
green  open   infra-000009
YN9EsULWSNaxWeeNvOs0RA   3 1      258799            0       337          168
green  open   infra-000014
YP0U6R7FQ_GVQVQZ6Yh9Ig   3 1      223788            0       292          146
green  open   infra-000015
JRBbAbEmSMqK5X40df9HbQ   3 1      224371            0       291          145
green  open   .orphaned.2020.06.30
n_xQC2dWQzConkvQqei3YA   3 1          9            0         0            0
green  open   infra-000007
llkkAVSzSOmosWTSAJM_hg   3 1      228584            0       296          148
green  open   infra-000005
d9BoGQdiQASsS3BBFm2iRA   3 1      227987            0       297          148
green  open   infra-000003                                                1-
goREK1QUKlQPAIVkWVaQ   3 1      226719            0       295          147
green  open   .security
zeT65uOuRTKZMjg_bbUc1g   1 1          5            0         0            0
green  open   .kibana-377444158_kubeadmin                                 wvMhDwJkR-
mRZQO84K0gUQ   3 1          1            0         0            0
green  open   infra-000006                                               5H-
KBSXGQKiO7hdapDE23g   3 1      226676            0       295          147
green  open   infra-000001                                               eH53BQ-
bSxSWR5xYZB6lVg   3 1      341800            0       443          220
green  open   .kibana-6
RVp7TemSSemGJcsSUmuf3A   1 1          4            0         0            0
green  open   infra-000011
J7XWBauWSTe0jnzX02fU6A   3 1      226100            0       293          146
green  open   app-000001
axSAFfONQDmKwatkjPXdtw   3 1      103186            0       126           57
green  open   infra-000016
m9c1iRLtStWSF1GopaRyCg   3 1       13685            0        19            9
green  open   infra-000002                                               Hz6WvINtTvKcQzw-
ewmbYg   3 1      228994            0       296          148
green  open   infra-000013                                               KR9mMFUpQl-
jraYtanyIGw   3 1      228166            0       298          148
green  open   audit-000001
eERqLdLmQOiQDFES1LBATQ   3 1          0            0         0            0
```

e. ログコレクターが 4.5 に更新されていることを確認します。

```
$ oc get ds fluentd -o json | grep fluentd-init
```

出力に **fluentd-init** コンテナーが含まれていることを確認します。

```
"containerName": "fluentd-init"
```

f. Kibana CRD を使用してログビジュアライザーが 4.5 に更新されていることを確認します。

```
$ oc get kibana kibana -o json
```

出力に **ready** ステータスの Kibana Pod が含まれることを確認します。

例8.2 準備状態にある Kibana Pod の出力例

```
[
{
"clusterCondition": {
"kibana-5fdd766ffd-nb2jj": [
{
"lastTransitionTime": "2020-06-30T14:11:07Z",
"reason": "ContainerCreating",
"status": "True",
"type": ""
},
{
"lastTransitionTime": "2020-06-30T14:11:07Z",
"reason": "ContainerCreating",
"status": "True",
"type": ""
}
]
},
"deployment": "kibana",
"pods": {
"failed": [],
"notReady": []
"ready": []
},
"replicaSets": [
"kibana-5fdd766ffd"
],
"replicas": 1
}
]
```

g. Curator が 4.5 に更新されていることを確認します。

```
$ oc get cronjob -o name
```

```
cronjob.batch/curator
cronjob.batch/elasticsearch-delete-app
cronjob.batch/elasticsearch-delete-audit
cronjob.batch/elasticsearch-delete-infra
```

```
cronjob.batch/elasticsearch-rollover-app
cronjob.batch/elasticsearch-rollover-audit
cronjob.batch/elasticsearch-rollover-infra
```

出力に **elasticsearch-delete-*** および **elasticsearch-rollover-*** インデックスが含まれることを確認します。

8.1.1. 更新後のタスク

Kibana を使用する場合、Elasticsearch Operator および Cluster Logging Operator が完全に 4.5 に更新された後に、Kibana インデックスパターンおよびビジュアライゼーションを再作成する必要があります。セキュリティープラグインの変更により、クラスターロギングのアップグレードではインデックスパターンが自動的に作成されません。

8.2. KIBANA インデックスパターンの定義

インデックスパターンは、可視化する必要のある Elasticsearch インデックスを定義します。Kibana でデータを確認し、可視化するには、インデックスパターンを作成する必要があります。

前提条件

- Kibana で **infra** および **audit** インデックスを表示するには、ユーザーには **cluster-admin** ロール、 **cluster-reader** ロール、または両方のロールが必要です。デフォルトの **kubeadmin** ユーザーには、これらのインデックスを表示するための適切なパーミッションがあります。**default**、**kube-** および **openshift-** プロジェクトで Pod およびログを表示できる場合、これらのインデックスにアクセスできるはずです。以下のコマンドを使用して、現在のユーザーが適切なパーミッションを持っているかどうかを確認することができます。

```
$ oc auth can-i get pods/log -n <project>
```

出力例

```
yes
```

注記

監査ログは、デフォルトでは内部 OpenShift Container Platform Elasticsearch インスタンスに保存されません。Kibana で監査ログを表示するには、ログ転送 API を使用して監査ログの **default** 出力を使用するパイプラインを設定する必要があります。

- Elasticsearch ドキュメントは、インデックスパターンを作成する前にインデックス化する必要があります。これは自動的に実行されますが、新規または更新されたクラスターでは数分の時間がかかる可能性があります。

手順

Kibana でインデックスパターンを定義し、ビジュアライゼーションを作成するには、以下を実行します。

1. OpenShift Container Platform コンソールで、Application Launcher  をクリックし、**Logging** を選択します。

2. **Management → Index Patterns → Create index pattern** をクリックして Kibana インデックスパターンを作成します。

   - 各ユーザーは、プロジェクトのログを確認するために、Kibana に初めてログインする際にインデックスパターンを手動で作成する必要があります。ユーザーは **app** という名前のインデックスパターンを作成し、**@timestamp** 時間フィールドを使用してコンテナーログを表示する必要があります。

   - 管理ユーザーはそれぞれ、最初に Kibana にログインする際に、**@timestamp** 時間フィールドを使用して **app**、 **infra** および **audit** インデックスについてインデックスパターンを作成する必要があります。

3. 新規インデックスパターンから Kibana のビジュアライゼーション (Visualization) を作成します。

第9章 クラスターロギングのトラブルシューティング

9.1. クラスターロギングのステータス表示

Cluster Logging Operator のステータスや、数多くのクラスターロギングコンポーネントを表示できます。

9.1.1. Cluster Logging Operator のステータス表示

Cluster Logging Operator のステータスを表示することができます。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

1. **openshift-logging** プロジェクトに切り替えます。

```
$ oc project openshift-logging
```

2. クラスターロギングのステータスを表示するには、以下を実行します。

   a. クラスターロギングのステータスを取得します。

```
$ oc get clusterlogging instance -o yaml
```

出力例

```
apiVersion: logging.openshift.io/v1
kind: ClusterLogging

....

status: 1
  collection:
    logs:
      fluentdStatus:
        daemonSet: fluentd 2
        nodes:
          fluentd-2rhqp: ip-10-0-169-13.ec2.internal
          fluentd-6fgjh: ip-10-0-165-244.ec2.internal
          fluentd-6l2ff: ip-10-0-128-218.ec2.internal
          fluentd-54nx5: ip-10-0-139-30.ec2.internal
          fluentd-flpnn: ip-10-0-147-228.ec2.internal
          fluentd-n2frh: ip-10-0-157-45.ec2.internal
        pods:
          failed: []
          notReady: []
          ready:
          - fluentd-2rhqp
          - fluentd-54nx5
          - fluentd-6fgjh
```

```
        - fluentd-6l2ff
        - fluentd-flpnn
        - fluentd-n2frh
    logstore: 3
      elasticsearchStatus:
      - ShardAllocationEnabled:  all
        cluster:
          activePrimaryShards:    5
          activeShards:           5
          initializingShards:     0
          numDataNodes:           1
          numNodes:               1
          pendingTasks:           0
          relocatingShards:       0
          status:                 green
          unassignedShards:       0
        clusterName:              elasticsearch
        nodeConditions:
          elasticsearch-cdm-mkkdys93-1:
        nodeCount:  1
        pods:
          client:
            failed:
            notReady:
            ready:
            - elasticsearch-cdm-mkkdys93-1-7f7c6-mjm7c
          data:
            failed:
            notReady:
            ready:
            - elasticsearch-cdm-mkkdys93-1-7f7c6-mjm7c
          master:
            failed:
            notReady:
            ready:
            - elasticsearch-cdm-mkkdys93-1-7f7c6-mjm7c
    visualization: 4
      kibanaStatus:
      - deployment: kibana
        pods:
          failed: []
          notReady: []
          ready:
          - kibana-7fb4fd4cc9-f2nls
        replicaSets:
        - kibana-7fb4fd4cc9
        replicas: 1
```

1. 出力の **status** スタンザに、クラスターステータスのフィールドが表示されます。
2. Fluentd Pod についての情報
3. Elasticsearch クラスターの健全性 (**green**、**yellow**、または **red**) などの Elasticsearch Pod についての情報
4. Kibana Pod についての情報

9.1.1.1. 状態メッセージ (condition message) のサンプル

以下は、クラスターロギングインスタンスの **Status.Nodes** セクションからの一部の状態メッセージの例です。

以下のようなステータスメッセージは、ノードが設定された低基準値を超えており、シャードがこのノードに割り当てられないことを示します。

出力例

```
nodes:
- conditions:
  - lastTransitionTime: 2019-03-15T15:57:22Z
    message: Disk storage usage for node is 27.5gb (36.74%). Shards will be not
      be allocated on this node.
    reason: Disk Watermark Low
    status: "True"
    type: NodeStorage
  deploymentName: example-elasticsearch-clientdatamaster-0-1
  upgradeStatus: {}
```

以下のようなステータスメッセージは、ノードが設定された高基準値を超えており、シャードが他のノードに移動させられることを示します。

出力例

```
nodes:
- conditions:
  - lastTransitionTime: 2019-03-15T16:04:45Z
    message: Disk storage usage for node is 27.5gb (36.74%). Shards will be relocated
      from this node.
    reason: Disk Watermark High
    status: "True"
    type: NodeStorage
  deploymentName: cluster-logging-operator
  upgradeStatus: {}
```

以下のようなステータスメッセージは、CR の Elasticsearch ノードセレクターがクラスターのいずれのノードにも一致しないことを示します。

出力例

```
 Elasticsearch Status:
   Shard Allocation Enabled:  shard allocation unknown
   Cluster:
     Active Primary Shards:  0
     Active Shards:          0
     Initializing Shards:    0
     Num Data Nodes:         0
     Num Nodes:              0
     Pending Tasks:          0
     Relocating Shards:      0
     Status:                 cluster health unknown
     Unassigned Shards:      0
   Cluster Name:             elasticsearch
```

```
    Node Conditions:
      elasticsearch-cdm-mkkdys93-1:
        Last Transition Time:  2019-06-26T03:37:32Z
        Message:               0/5 nodes are available: 5 node(s) didn't match node selector.
        Reason:                Unschedulable
        Status:                True
        Type:                  Unschedulable
      elasticsearch-cdm-mkkdys93-2:
    Node Count:  2
    Pods:
      Client:
        Failed:
        Not Ready:
          elasticsearch-cdm-mkkdys93-1-75dd69dccd-f7f49
          elasticsearch-cdm-mkkdys93-2-67c64f5f4c-n58vl
        Ready:
      Data:
        Failed:
        Not Ready:
          elasticsearch-cdm-mkkdys93-1-75dd69dccd-f7f49
          elasticsearch-cdm-mkkdys93-2-67c64f5f4c-n58vl
        Ready:
      Master:
        Failed:
        Not Ready:
          elasticsearch-cdm-mkkdys93-1-75dd69dccd-f7f49
          elasticsearch-cdm-mkkdys93-2-67c64f5f4c-n58vl
        Ready:
```

以下のようなステータスメッセージは、要求された PVC が PV にバインドされないことを示します。

出力例

```
    Node Conditions:
      elasticsearch-cdm-mkkdys93-1:
        Last Transition Time:  2019-06-26T03:37:32Z
        Message:               pod has unbound immediate PersistentVolumeClaims (repeated 5 times)
        Reason:                Unschedulable
        Status:                True
        Type:                  Unschedulable
```

以下のようなステータスメッセージは、ノードセレクターがいずれのノードにも一致しないため、Fluentd Pod をスケジュールできないことを示します。

出力例

```
Status:
  Collection:
    Logs:
      Fluentd Status:
        Daemon Set:  fluentd
        Nodes:
        Pods:
```

```
    Failed:
    Not Ready:
    Ready:
```

9.1.2. クラスターロギングコンポーネントのステータスの表示

数多くのクラスターロギングコンポーネントのステータスを表示することができます。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

1. **openshift-logging** プロジェクトに切り替えます。

```
$ oc project openshift-logging
```

2. クラスターロギング環境のステータスを表示します。

```
$ oc describe deployment cluster-logging-operator
```

出力例

```
Name:                   cluster-logging-operator

....

Conditions:
  Type          Status  Reason
  ----          ------  ------
  Available     True    MinimumReplicasAvailable
  Progressing   True    NewReplicaSetAvailable

....

Events:
  Type    Reason             Age   From                    Message
  ----    ------             ----  ----                    -------
  Normal  ScalingReplicaSet  62m   deployment-controller  Scaled up replica set cluster-
logging-operator-574b8987df to 1----
```

3. クラスターロギングレプリカセットのステータスを表示します。

   a. レプリカセットの名前を取得します。

出力例

```
$ oc get replicaset
```

出力例

```
NAME                                  DESIRED   CURRENT   READY   AGE
```

```
cluster-logging-operator-574b8987df       1         1         1       159m
elasticsearch-cdm-uhr537yu-1-6869694fb    1         1         1       157m
elasticsearch-cdm-uhr537yu-2-857b6d676f   1         1         1       156m
elasticsearch-cdm-uhr537yu-3-5b6fdd8cfd   1         1         1       155m
kibana-5bd5544f87                         1         1         1       157m
```

b. レプリカセットのステータスを取得します。

```
$ oc describe replicaset cluster-logging-operator-574b8987df
```

出力例

```
Name:           cluster-logging-operator-574b8987df

....

Replicas:       1 current / 1 desired
Pods Status:    1 Running / 0 Waiting / 0 Succeeded / 0 Failed

....

Events:
  Type    Reason            Age   From                   Message
  ----    ------            ----  ----                   -------
  Normal  SuccessfulCreate  66m   replicaset-controller  Created pod: cluster-logging-
operator-574b8987df-qjhqv----
```

9.2. ログストアのステータスの表示

Elasticsearch Operator のステータスや、数多くの Elasticsearch コンポーネントを表示できます。

9.2.1. ログストアのステータスの表示

ログストアのステータスを表示することができます。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

1. **openshift-logging** プロジェクトに切り替えます。

```
$ oc project openshift-logging
```

2. ステータスを表示するには、以下を実行します。

a. ログストアインスタンスの名前を取得します。

```
$ oc get Elasticsearch
```

出力例

```
```

```
NAME          AGE
elasticsearch   5h9m
```

b. ログストアのステータスを取得します。

```
$ oc get Elasticsearch <Elasticsearch-instance> -o yaml
```

以下に例を示します。

```
$ oc get Elasticsearch elasticsearch -n openshift-logging -o yaml
```

出力には、以下のような情報が含まれます。

出力例

```
status: 1
  cluster: 2
    activePrimaryShards: 30
    activeShards: 60
    initializingShards: 0
    numDataNodes: 3
    numNodes: 3
    pendingTasks: 0
    relocatingShards: 0
    status: green
    unassignedShards: 0
  clusterHealth: ""
  conditions: [] 3
  nodes: 4
  - deploymentName: elasticsearch-cdm-zjf34ved-1
    upgradeStatus: {}
  - deploymentName: elasticsearch-cdm-zjf34ved-2
    upgradeStatus: {}
  - deploymentName: elasticsearch-cdm-zjf34ved-3
    upgradeStatus: {}
  pods: 5
    client:
      failed: []
      notReady: []
      ready:
      - elasticsearch-cdm-zjf34ved-1-6d7fbf844f-sn422
      - elasticsearch-cdm-zjf34ved-2-dfbd988bc-qkzjz
      - elasticsearch-cdm-zjf34ved-3-c8f566f7c-t7zkt
    data:
      failed: []
      notReady: []
      ready:
      - elasticsearch-cdm-zjf34ved-1-6d7fbf844f-sn422
      - elasticsearch-cdm-zjf34ved-2-dfbd988bc-qkzjz
      - elasticsearch-cdm-zjf34ved-3-c8f566f7c-t7zkt
    master:
      failed: []
      notReady: []
      ready:
```

```
    - elasticsearch-cdm-zjf34ved-1-6d7fbf844f-sn422
    - elasticsearch-cdm-zjf34ved-2-dfbd988bc-qkzjz
    - elasticsearch-cdm-zjf34ved-3-c8f566f7c-t7zkt
  shardAllocationEnabled: all
```

1. 出力の **status** スタンザに、クラスターステータスのフィールドが表示されます。
2. ログストアのステータス:
   - アクティブなプライマリーシャードの数
   - アクティブなシャードの数
   - 初期化されるシャードの数
   - ログストアデータノードの数。
   - ログストアノードの合計数。
   - 保留中のタスクの数。
   - ログストアのステータス: **green**、**red**、**yellow**。
   - 未割り当てのシャードの数。
3. ステータス状態 (ある場合)。ログストアのステータスは、Pod が配置されていない場合にスケジューラーからの理由を示します。以下の状況に関連したイベントが表示されます。
   - ログストアおよびプロキシーコンテナーの両方についてコンテナーが待機中。
   - ログストアおよびプロキシーコンテナーの両方についてコンテナーが終了している。
   - Pod がスケジュール対象外である。さらに多数の問題についての状態が表示されます。詳細は、**状態メッセージのサンプル** を参照してください。
4. **upgradeStatus** のあるクラスター内のログストアノード。
5. 'failed`、**notReady** または **ready** 状態の下に一覧表示された、クラスター内のログストアクライアント、データ、およびマスター Pod。

9.2.1.1. 状態メッセージ (condition message) のサンプル

以下は、Elasticsearch インスタンスの **Status** セクションからの一部の状態メッセージの例になります。

このステータスメッセージは、ノードが設定された低基準値を超えており、シャードがこのノードに割り当てられないことを示します。

```
status:
  nodes:
  - conditions:
    - lastTransitionTime: 2019-03-15T15:57:22Z
      message: Disk storage usage for node is 27.5gb (36.74%). Shards will be not
        be allocated on this node.
```

```
      reason: Disk Watermark Low
      status: "True"
      type: NodeStorage
    deploymentName: example-elasticsearch-cdm-0-1
    upgradeStatus: {}
```

このステータスメッセージは、ノードが設定された高基準値を超えており、シャードが他のノードに移動させられることを示します。

```
status:
  nodes:
  - conditions:
    - lastTransitionTime: 2019-03-15T16:04:45Z
      message: Disk storage usage for node is 27.5gb (36.74%). Shards will be relocated
        from this node.
      reason: Disk Watermark High
      status: "True"
      type: NodeStorage
    deploymentName: example-elasticsearch-cdm-0-1
    upgradeStatus: {}
```

このステータスメッセージは、CR のログストアノードセレクターがクラスターのいずれのノードにも一致しないことを示します。

```
status:
    nodes:
    - conditions:
      - lastTransitionTime: 2019-04-10T02:26:24Z
        message: '0/8 nodes are available: 8 node(s) didn''t match node selector.'
        reason: Unschedulable
        status: "True"
        type: Unschedulable
```

このステータスメッセージは、ログストア CR が存在しない PVC を使用することを示します。

```
status:
  nodes:
  - conditions:
    - last Transition Time:  2019-04-10T05:55:51Z
      message:               pod has unbound immediate PersistentVolumeClaims (repeated 5 times)
      reason:                Unschedulable
      status:                True
      type:                  Unschedulable
```

このステータスメッセージは、ログストアクラスターにはログストアの冗長性ポリシーをサポートするための十分なノードがないことを示します。

```
status:
  clusterHealth: ""
  conditions:
  - lastTransitionTime: 2019-04-17T20:01:31Z
    message: Wrong RedundancyPolicy selected. Choose different RedundancyPolicy or
      add more nodes with data roles
```

```
    reason: Invalid Settings
    status: "True"
    type: InvalidRedundancy
```

このステータスメッセージは、クラスター内のマスターノードの数が多過ぎることを示します。

```
status:
  clusterHealth: green
  conditions:
    - lastTransitionTime: '2019-04-17T20:12:34Z'
      message: >-
        Invalid master nodes count. Please ensure there are no more than 3 total
        nodes with master roles
      reason: Invalid Settings
      status: 'True'
      type: InvalidMasters
```

9.2.2. ログストアコンポーネントのステータスの表示

数多くのログストアコンポーネントのステータスを表示することができます。

Elasticsearch インデックス

Elasticsearch インデックスのステータスを表示することができます。

1. Elasticsearch Pod の名前を取得します。

```
$ oc get pods --selector component=elasticsearch -o name
```

出力例

```
pod/elasticsearch-cdm-1godmszn-1-6f8495-vp4lw
pod/elasticsearch-cdm-1godmszn-2-5769cf-9ms2n
pod/elasticsearch-cdm-1godmszn-3-f66f7d-zqkz7
```

2. インデックスのステータスを取得します。

```
$ oc exec elasticsearch-cdm-4vjor49p-2-6d4d7db474-q2w7z -- indices
```

出力例

```
Defaulting container name to elasticsearch.
Use 'oc describe pod/elasticsearch-cdm-4vjor49p-2-6d4d7db474-q2w7z -n openshift-
logging' to see all of the containers in this pod.

green  open   infra-000002                                    S4QANnf1QP6NgCegfnrnbQ
3   1     119926            0       157            78
green  open   audit-000001                                    8_EQx77iQCSTzFOXtxRqFw
3   1          0            0         0             0
green  open   .security                                       iDjscH7aSUGhIdq0LheLBQ   1
1          5            0         0             0
green  open   .kibana_-377444158_kubeadmin
yBywZ9GfSrKebz5gWBZbjw   3   1          1            0         0             0
green  open   infra-000001                                    z6Dpe__ORgiopEpW6Yl44A
```

```
3   1     871000          0       874          436
green  open   app-000001                                  hIrazQCeSISewG3c2VIvsQ
3   1      2453          0        3           1
green  open   .kibana_1                                   JCitcBMSQxKOvIq6iQW6wg
1   1         0          0        0           0
green  open   .kibana_-1595131456_user1                        gIYFIEGRRe-
ka0W3okS-mQ   3   1         1          0        0           0
```

ログストア Pod

ログストアをホストする Pod のステータスを表示することができます。

1. Pod の名前を取得します。

```
$ oc get pods --selector component=elasticsearch -o name
```

出力例

```
pod/elasticsearch-cdm-1godmszn-1-6f8495-vp4lw
pod/elasticsearch-cdm-1godmszn-2-5769cf-9ms2n
pod/elasticsearch-cdm-1godmszn-3-f66f7d-zqkz7
```

2. Pod のステータスを取得します。

```
$ oc describe pod elasticsearch-cdm-1godmszn-1-6f8495-vp4lw
```

出力には、以下のようなステータス情報が含まれます。

出力例

```
....
Status:             Running

....

Containers:
  elasticsearch:
    Container ID:   cri-o://b7d44e0a9ea486e27f47763f5bb4c39dfd2
    State:          Running
      Started:      Mon, 08 Jun 2020 10:17:56 -0400
    Ready:          True
    Restart Count:  0
    Readiness:  exec [/usr/share/elasticsearch/probe/readiness.sh] delay=10s timeout=30s
period=5s #success=1 #failure=3

....

  proxy:
    Container ID:  cri-
o://3f77032abaddbb1652c116278652908dc01860320b8a4e741d06894b2f8f9aa1
    State:          Running
      Started:      Mon, 08 Jun 2020 10:18:38 -0400
    Ready:          True
    Restart Count:  0
```

```
....

Conditions:
  Type              Status
  Initialized       True
  Ready             True
  ContainersReady   True
  PodScheduled      True

....

Events:         <none>
```

ログストレージ Pod デプロイメント設定

ログストアのデプロイメント設定のステータスを表示することができます。

1. デプロイメント設定の名前を取得します。

```
$ oc get deployment --selector component=elasticsearch -o name
```

出力例

```
deployment.extensions/elasticsearch-cdm-1gon-1
deployment.extensions/elasticsearch-cdm-1gon-2
deployment.extensions/elasticsearch-cdm-1gon-3
```

2. デプロイメント設定のステータスを取得します。

```
$ oc describe deployment elasticsearch-cdm-1gon-1
```

出力には、以下のようなステータス情報が含まれます。

出力例

```
....
  Containers:
   elasticsearch:
    Image:      registry.redhat.io/openshift4/ose-logging-elasticsearch5:v4.3
    Readiness:  exec [/usr/share/elasticsearch/probe/readiness.sh] delay=10s timeout=30s
period=5s #success=1 #failure=3

....

Conditions:
  Type          Status   Reason
  ----          ------   ------
  Progressing    Unknown  DeploymentPaused
  Available      True     MinimumReplicasAvailable

....

Events:         <none>
```

ログストアのレプリカセット

ログストアのレプリカセットのステータスを表示することができます。

1. レプリカセットの名前を取得します。

```
$ oc get replicaSet --selector component=elasticsearch -o name

replicaset.extensions/elasticsearch-cdm-1gon-1-6f8495
replicaset.extensions/elasticsearch-cdm-1gon-2-5769cf
replicaset.extensions/elasticsearch-cdm-1gon-3-f66f7d
```

2. レプリカセットのステータスを取得します。

```
$ oc describe replicaSet elasticsearch-cdm-1gon-1-6f8495
```

出力には、以下のようなステータス情報が含まれます。

出力例

```
....
  Containers:
   elasticsearch:
    Image:      registry.redhat.io/openshift4/ose-logging-
elasticsearch6@sha256:4265742c7cdd85359140e2d7d703e4311b6497eec7676957f455d6
908e7b1c25
    Readiness:  exec [/usr/share/elasticsearch/probe/readiness.sh] delay=10s timeout=30s
period=5s #success=1 #failure=3

....

Events:         <none>
```

9.3. クラスターロギングのアラートについて

ロギングコレクターのアラートはすべて、OpenShift Container Platform Web コンソールの Alerting UI に一覧表示されます。

9.3.1. ロギングコレクターアラートの表示

アラートは、OpenShift Container Platform Web コンソールの、Alerting UI の **Alerts** タブに表示されます。アラートは以下の状態のいずれかになります。

- **Firing**アラートの状態はタイムアウトの期間は true になります。Firing アラートの末尾の **Option** メニューをクリックし、詳細情報を表示するか、アラートを非通知 (silence) にします。
- **Pending**: このアラート状態は現時点で true ですが、タイムアウトに達していません。
- **Not Firing**アラートは現時点でトリガーされていません。

手順

クラスターロギングおよびその他の OpenShift Container Platform アラートを表示するには、以下を実行します。

1. OpenShift Container Platform コンソールで、**Monitoring → Alerting** をクリックします。
2. **Alerts** タブをクリックします。選択したフィルターに基づいてアラートが一覧表示されます。

追加リソース

- Alerting UI の詳細は、クラスターアラートの管理 を参照してください。

9.3.2. ロギングコレクターのアラートについて

以下のアラートはロギングコレクターによって生成されます。これらのアラートは、OpenShift Container Platform Web コンソールの Alerting UI の **Alerts** ページで表示できます。

表9.1 Fluentd Prometheus アラート

アラート	メッセージ	説明	重大度
FluentdErrorsHigh	**In the last minute, <value> errors reported by fluentd <instance>.**	Fluentd は指定した数 (デフォルトでは 10) よりも多くの問題を報告しています。	Critical
FluentdNodeDown	**Prometheus could not scrape fluentd <instance> for more than 10m.**	Fluentd は Prometheus が特定の Fluentd インスタンスを収集できなかったことを報告します。	Critical
FluentdQueueLengthBurst	**In the last minute, fluentd <instance> buffer queue length increased more than 32.Current value is <value>.**	Fluentd は値が大きすぎることを報告しています。	Warning
FluentdQueueLengthIncreasing	**In the last 12h, fluentd <instance> buffer queue length constantly increased more than 1.Current value is <value>.**	Fluentd はキューの使用についての問題を報告しています。	Critical

9.3.3. Elasticsearch アラートルール

これらのアラートルールを Prometheus に表示できます。

アラート	説明	重大度

アラート	説明	重大度
ElasticsearchClusterNotHealthy	クラスターのヘルスステータスは少なくとも 2m の間 RED になります。クラスターは書き込みを受け入れず、シャードが見つからない可能性があるか、またはマスターノードがまだ選択されていません。	critical
ElasticsearchClusterNotHealthy	クラスターのヘルスステータスは少なくとも 20m の間 YELLOW になります。一部のシャードレプリカは割り当てられません。	warning
ElasticsearchBulkRequestsRejectionJumps	クラスターのノードにおける高いバルク除去率 (High Bulk Rejection Ratio) を示します。このノードはインデックスの速度に追い付いていない可能性があります。	warning
ElasticsearchNodeDiskWatermarkReached	クラスターのノードでディスクの低い基準値に達しています。シャードをこのノードに割り当てることはできません。ノードにディスク領域を追加することを検討する必要があります。	alert
ElasticsearchNodeDiskWatermarkReached	クラスターのノードでディスクの高い基準値に達しています。一部のシャードは可能な場合に別のノードに再度割り当てられる可能性があります。ノードにディスク領域が追加されるか、またはこのノードに割り当てられる古いインデックスをドロップします。	high
ElasticsearchJVMHeapUseHigh	クラスター内のノード上での JVM ヒープの使用量は <value> です。	alert
AggregatedLoggingSystemCPUHigh	クラスター内のノード上でのシステム CPU の使用量は <value> です。	alert
ElasticsearchProcessCPUHigh	クラスター内のノード上での ES プロセス CPU の使用量は <value> です。	alert

9.4. ログキュレーターのトラブルシューティング

本セクションの情報を使用してログ収集のデバッグを実行できます。Curator は、OpenShift Container Platform 4.5 より前には Elasticsearch インデックス形式にあるデータを削除するために使用されましたが、今後のリリースでは削除されます。

9.4.1. ログ収集のトラブルシューティング

本セクションの情報を使用してログ収集のデバッグを実行できます。たとえば、Curator が失敗状態にあり、ログメッセージで理由が示されていない場合、次にスケジュールされている cron ジョブの実行を待機する代わりに、ログレベルを引き上げ、新規ジョブをトリガーできます。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

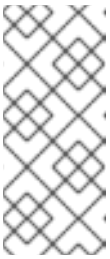
Curator のデバッグログを有効にし、次の Curator の反復を手動でトリガーするには、以下を実行します。

1. Curator のデバッグログを有効にします。

```
$ oc set env cronjob/curator CURATOR_LOG_LEVEL=DEBUG
CURATOR_SCRIPT_LOG_LEVEL=DEBUG
```

ログレベルを指定します。

- **CRITICAL**。Curator は重大なメッセージのみを表示します。
- **ERROR**。Curator はエラーおよび重大なメッセージのみを表示します。
- **WARNING**。Curator はエラー、警告、および重大なメッセージのみを表示します。
- **INFO**。Curator は情報、エラー、警告、および重大なメッセージのみを表示します。
- **DEBUG**。Curator は上記のすべてに加えてデバッグメッセージのみを表示します。デフォルト値は INFO です。



注記

クラスターロギングは、OpenShift Container Platform ラッパースクリプト (**run.sh** および **convert.py**) で OpenShift Container Platform カスタム環境変数 **CURATOR_SCRIPT_LOG_LEVEL** を使用します。この環境変数は、必要に応じてスクリプトのデバッグ用に **CURATOR_LOG_LEVEL** と同じ値を取ります。

2. 次の Curator の反復をトリガーします。

```
$ oc create job --from=cronjob/curator <job_name>
```

3. 以下のコマンドを使用して cron ジョブを制御します。

- cron ジョブを一時停止します。

```
$ oc patch cronjob curator -p '{"spec":{"suspend":true}}'
```

- cron ジョブを再開します。

```
$ oc patch cronjob curator -p '{"spec":{"suspend":false}}'
```

- cron ジョブスケジュールを変更します。

```
$ oc patch cronjob curator -p '{"spec":{"schedule":"0 0 * * *"}}' 1
```

1 **schedule** オプションは、cron 形式 のスケジュールを受け入れます。

9.5. RED HAT サポート用のロギングデータの収集

サポートケースを作成する際、ご使用のクラスターについてのデバッグ情報を Red Hat サポートに提供していただくと Red Hat のサポートに役立ちます。

must-gather ツール を使用すると、プロジェクトレベルのリソース、クラスターレベルのリソース、および各クラスターロギングコンポーネントについての診断情報を収集できます。

迅速なサポートを得るには、OpenShift Container Platform とクラスターロギングの両方の診断情報を提供してください。

注記

hack/logging-dump.sh スクリプトは使用しないでください。このスクリプトはサポートされなくなり、データを収集しません。

9.5.1. must-gather ツールについて

oc adm must-gather CLI コマンドは、問題のデバッグに必要となる可能性のあるクラスターからの情報を収集します。

クラスターロギング環境の場合、**must-gather** は以下の情報を収集します。

- プロジェクトレベルの Pod、設定マップ、サービスアカウント、ロール、ロールバインディングおよびイベントを含むプロジェクトレベルのリソース
- クラスターレベルでのノード、ロール、およびロールバインディングを含むクラスターレベルのリソース
- ログコレクター、ログストア、curator、およびログビジュアライザーなどの **openshift-logging** および **openshift-operators-redhat** namespace のクラスターロギングリソース

oc adm must-gather を実行すると、新しい Pod がクラスターに作成されます。データは Pod で収集され、**must-gather.local** で始まる新規ディレクトリーに保存されます。このディレクトリーは、現行の作業ディレクトリーに作成されます。

9.5.2. 前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

9.5.3. クラスターロギングデータの収集

oc adm must-gather CLI コマンドを使用して、クラスターロギング環境についての情報を収集できます。

手順

must-gather でクラスターロギング情報を収集するには、以下を実行します。

1. **must-gather** 情報を保存する必要のあるディレクトリーに移動します。
2. クラスターロギングイメージに対して **oc adm must-gather** コマンドを実行します。

```
$ oc adm must-gather --image=$(oc -n openshift-logging get deployment.apps/cluster-logging-operator -o jsonpath='{.spec.template.spec.containers[?(@.name == "cluster-logging-operator")].image}')
```

must-gather ツールは、現行ディレクトリー内の **must-gather.local** で始まる新規ディレクトリーを作成します。例: **must-gather.local.4157245944708210408**

3. 作成された **must-gather** ディレクトリーから圧縮ファイルを作成します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ tar -cvaf must-gather.tar.gz must-gather.local.4157245944708210408
```

4. 圧縮ファイルを Red Hat カスタマーポータル で作成したサポートケースに添付します。

第10章 クラスターロギングのアンインストール

クラスターロギングをお使いの OpenShift Container Platform クラスターから削除することができます。

10.1. OPENSHIFT CONTAINER PLATFORM からのクラスターロギングのアンインストール

ClusterLogging カスタムリソース (CR) を削除して、ログ集計を停止できます。ただし、CR の削除後に残る他のクラスターロギングコンポーネントがあり、これらはオプションで削除できます。

前提条件

- クラスターロギングおよび Elasticsearch がインストールされている。

手順

クラスターロギングを削除するには、以下を実行します。

1. OpenShift Container Platform Web コンソールを使って **ClusterLogging** CR を削除できます。
   a. **Administration → Custom Resource Definitions**ページに切り替えます。
   b. **Custom Resource Definitions**ページで、**ClusterLogging** をクリックします。
   c. **Custom Resource Definition Details**ページで、 **Instances** をクリックします。
   d. インスタンスの横にある Options メニュー  をクリックし、 **Delete ClusterLogging** を選択します。
2. オプション: カスタムリソース定義 (CRD) を削除します。
   a. **Administration → Custom Resource Definitions**ページに切り替えます。
   b. **ClusterLogging** の横にある Options メニュー  をクリックし、 **Delete Custom Resource Definition** を選択します。
   c. **Elasticsearch** の横にある Options メニュー  をクリックし、**Delete Custom Resource Definition** を選択します。
   d. **LogForwarding** の横にある Options メニュー  をクリックし、 **Delete Custom Resource Definition** を選択します。
3. オプション: Cluster Logging Operator および Elasticsearch Operator を削除します。
   a. **Operators → Installed Operators** ページに切り替えます。
   b. **openshift-logging** プロジェクトを選択します。

c. Cluster Logging Operator の横にある Options メニュー をクリックし、**Uninstall Operator** を選択します。

d. **openshift-operators-redhat** プロジェクトを選択します。

e. Elasticsearch Operator の横にある Options メニュー をクリックし、**Uninstall Operator** を選択します。

4. オプション: Cluster Logging および Elasticsearch プロジェクト。

a. **Home → Projects** ページに切り替えます。

b. **openshift-logging** プロジェクトの横にある Options メニュー をクリックし、**Delete Project** を選択します。

c. ダイアログボックスで **openshift-logging** を入力して、**Delete** をクリックし、削除を確認します。

d. **openshift-operators-redhat** プロジェクトの横にある Options メニュー をクリックし、**Delete Project** を選択します。

重要

他のグローバル Operator がこの namespace にインストールされている場合、**openshift-operators-redhat** プロジェクトを削除しないでください。

e. ダイアログボックスで **openshift-operators-redhat** を入力し、**Delete** をクリックして削除を確認します。

第11章 エクスポートされるフィールド

ロギングシステムによってエクスポートされ、Elasticsearch および Kibana での検索に利用できるフィールドがあります。検索時には、ドットの付いたフィールドのフルネームを使用します。たとえば、Elasticsearch **/_search URL** の場合、Kubernetes Pod 名を検索するには、**/_search/q=kubernetes.pod_name:name-of-my-pod** を使用します。

以下のセクションでは、ロギングストアに存在しない可能性のあるフィールドについて説明します。これらのフィールドのすべてがすべてのレコードにある訳ではありません。フィールドは以下のカテゴリーに分類されます。

- **exported-fields-Default**
- **exported-fields-systemd**
- **exported-fields-kubernetes**
- **exported-fields-pipeline_metadata**
- **exported-fields-ovirt**
- **exported-fields-aushape**
- **exported-fields-tlog**

11.1. デフォルトのエクスポートされるフィールド

これらは、ロギングシステムによってエクスポートされるデフォルトフィールドであり、Elasticsearch および Kibana での検索に利用できます。デフォルトフィールドは最上位および **collectd*** フィールドです。

最上位フィールド
最上位フィールドは、すべてのアプリケーションに共通であり、すべてのレコードに存在する可能性があります。Elasticsearch テンプレートの場合、最上位フィールドは、テンプレートのマッピングセクションで **default** の実際のマッピングを設定します。

パラメーター	説明
@timestamp	ログペイロードが作成された時点か、作成時間が不明な場合はログペイロードが最初に収集された時点の UTC 値のマーキング。これは、ログを処理するパイプラインのログペイロードの生成時についてのベストエフォートベースの判別に基づきます。フィールドを特定の目的のために予約されることを示す **@** 接頭辞を追加します。Elasticsearch の場合、ほとんどのツールはデフォルトで **@timestamp** を検索します。形式は 2015-01-24 14:06:05.071000 などのようになります。
geoip	これはマシンの geo IP です。
hostname	**hostname** は、元のペイロードを生成するエンティティーの完全修飾ドメイン名 (FQDN) です 。このフィールドでは、このコンテキストの取得が試行されます。これを生成するエンティティーがコンテキストを認識している場合があります。また、エンティティーには、コレクターまたはノーマライザーによって認識される制限された namespace がある場合もあります。

パラメーター	説明
ipaddr4	ソースサーバーの IP アドレス V4。配列である場合があります。
ipaddr6	ソースサーバーの IP アドレス V6(ある場合)。
level	rsyslog (severitytext プロパティー)、python のロギングモジュールによって提供されるロギングレベル。使用できる値は **misc/sys/syslog.h** に一覧表示される値と、**trace** および **unknown** です。たとえば "alert crit debug emerg err info notice trace unknown warning" などがあります。**trace** は **syslog.h** 一覧にはありませんが、数多くのアプリケーションがこれを使用することに注意してください。 をクリックします。**unknown** は、ロギングシステムが認識しない値を取得した時にのみ使用します。この値は最も高い値であることに注意してください。**trace** は **debug** よりも高レベルで、詳細度が高いと見なされます。**error** の使用は推奨されていません。**err** を使用してください。**panic** を **emerg** に変換します。**warn** を **warning** に変換します。 **syslog/journal PRIORITY** からの数値は通常、misc/sys/syslog.h に記載されている優先順位の値を使用してマップされます。 他のロギングシステムからのログレベルおよび優先順位は、最も近い一致にマップされる必要があります。例については、python logging を参照してください。
message	通常のログエントリーメッセージまたはペイロードです。これはコレクターまたはノーマライザーによってプルされるメタデータから削除される可能性があります。これは UTF-8 でエンコーディングされます。
pid	ロギングエンティティーのプロセス ID です (ある場合)。
service	ロギングエンティティーに関連付けられたサービスの名前です (ある場合)。たとえば、**syslog APP-NAME** プロパティーは、サービスフィールドにマップされます。
tags	コレクターまたはノーマライザーによって各ログに配置される、オプションで指定される Operator 定義のタグの一覧です。ペイロードには、ホワイトスペースで区切られた文字列トークンまたは文字列トークンの JSON 一覧を使用した文字列を指定できます。
file	ファイルパスのコレクター **TODO** アナライザーに対してローカルのログエントリーを含むファイルへのオプションのパスです。

パラメーター	説明
offset	オフセット値では、値が単一ログファイルで単調に増加する場合に、バイトの値をファイルのログ行 (ゼロまたは 1 ベース) またはログ行の番号 (ゼロまたは 1 ベース) の開始地点に表示できます。この値はラップでき、ログファイルの新規バージョンを表示できます (ローテーション)。
namespace_name	このレコードを、その名前を共有する **namespace** に関連付けます。この値は保存されませんが、アクセス制御および可視化のためにレコードを適切な **namespace** に関連付けるために使用されます。通常、この値はタグに指定されますが、プロトコルがタグの送信をサポートしない場合、このフィールドを使用できます。このフィールドがある場合、これはタグまたは **kubernetes.namespace_name** に指定される **namespace** を上書きします。
namespace_uuid	これは、**namespace_name** に関連付けられる **uuid** です。この値は保存されませんが、アクセス制御および可視化のためにレコードを適切な namespace に関連付けるために使用されます。このフィールドがある場合、これは **kubernetes.namespace_uuid** に指定される **uuid** を上書きします。また、これにより、このログレコードの Kubernetes メタデータ検索はスキップされます。

collectd フィールド
以下のフィールドは namespace メトリクスのメタデータを表します。

パラメーター	説明
collectd.interval	type: float **collectd** の間隔。
collectd.plugin	type: string **collectd** プラグイン。
collectd.plugin_instance	type: string **collectd** plugin_instance
collectd.type_instance	type: string **collectd type_instance**。
collectd.type	type: string **collectd** タイプ。

パラメーター	説明
collectd.dstypes	type: string **collectd** データセットタイプ。

collectd.processes フィールド
以下のフィールドは **collectd** プロセスのプラグインに対応します。

パラメーター	説明
collectd.processes.ps_state	type: integer **collectd ps_state** タイプのプロセスプラグイン。

collectd.processes.ps_disk_ops フィールド
collectd ps_disk_ops タイプのプロセスプラグイン。

パラメーター	説明
collectd.processes.ps_disk_ops.read	type: float **TODO**
collectd.processes.ps_disk_ops.write	type: float **TODO**
collectd.processes.ps_vm	type: integer **collectd ps_vm** タイプのプロセスプラグイン。
collectd.processes.ps_rss	type: integer **collectd ps_rss** タイプのプロセスプラグイン。
collectd.processes.ps_data	type: integer **collectd ps_data** タイプのプロセスプラグイン。
collectd.processes.ps_code	type: integer **collectd ps_code** タイプのプロセスプラグイン。
collectd.processes.ps_stacksize	type: integer **collectd ps_stacksize** タイプのプロセスプラグイン。

collectd.processes.ps_cputime フィールド
collectd ps_cputime タイプのプロセスプラグイン。

パラメーター	説明
collectd.processes.ps_cputime.user	type: float **TODO**
collectd.processes.ps_cputime.syst	type: float **TODO**

collectd.processes.ps_count フィールド
collectd ps_count タイプのプロセスプラグイン。

パラメーター	説明
collectd.processes.ps_count.processes	type: integer **TODO**
collectd.processes.ps_count.threads	type: integer **TODO**

collectd.processes.ps_pagefaults フィールド
collectd ps_pagefaults タイプのプロセスプラグイン。

パラメーター	説明
collectd.processes.ps_pagefaults.majflt	type: float **TODO**
collectd.processes.ps_pagefaults.minflt	type: float **TODO**

collectd.processes.ps_disk_octets フィールド
collectd ps_disk_octets タイプのプロセスプラグイン。

パラメーター	説明
collectd.processes.ps_disk_octets.read	type: float **TODO**
collectd.processes.ps_disk_octets.write	type: float **TODO**

パラメーター	説明
collectd.processes.fork_rate	type: float **collectd fork_rate** タイプのプロセスプラグイン。

collectd.disk フィールド
collectd ディスクプラグインに対応します。

collectd.disk.disk_merged フィールド
collectd disk_merged タイプのディスクプラグイン。

パラメーター	説明
collectd.disk.disk_merged.read	type: float **TODO**
collectd.disk.disk_merged.write	type: float **TODO**

collectd.disk.disk_octets フィールド
collectd disk_octets タイプのディスクプラグイン。

パラメーター	説明
collectd.disk.disk_octets.read	type: float **TODO**
collectd.disk.disk_octets.write	type: float **TODO**

collectd.disk.disk_time フィールド
collectd disk_time タイプのディスクプラグイン。

パラメーター	説明
collectd.disk.disk_time.read	type: float **TODO**
collectd.disk.disk_time.write	type: float **TODO**

collectd.disk.disk_ops フィールド
collectd disk_ops タイプのディスクプラグインです。

パラメーター	説明
collectd.disk.disk_ops.read	type: float **TODO**
collectd.disk.disk_ops.write	type: float **TODO**
collectd.disk.pending_operations	type: integer **collectd pending_operations** タイプのディスクプラグイン。

collectd.disk.disk_io_time フィールド
collectd disk_io_time タイプのディスクプラグイン。

パラメーター	説明
collectd.disk.disk_io_time.io_time	type: float **TODO**
collectd.disk.disk_io_time.weighted_io_time	type: float **TODO**

collectd.interface フィールド
collectd インターフェイスプラグインに対応します。

collectd.interface.if_octets フィールド
collectd if_octets タイプのインターフェイスプラグイン。

パラメーター	説明
collectd.interface.if_octets.rx	type: float **TODO**
collectd.interface.if_octets.tx	type: float **TODO**

collectd.interface.if_packets フィールド
collectd if_packets タイプのインターフェイスプラグイン。

パラメーター	説明
collectd.interface.if_packets.rx	type: float **TODO**
collectd.interface.if_packets.tx	type: float **TODO**

collectd.interface.if_errors フィールド
collectd if_errors タイプのインターフェイスプラグイン。

パラメーター	説明
collectd.interface.if_errors.rx	type: float **TODO**
collectd.interface.if_errors.tx	type: float **TODO**

collectd.interface.if_dropped フィールド
collectd if_dropped タイプのインターフェイスプラグイン。

パラメーター	説明
collectd.interface.if_dropped.rx	type: float **TODO**
collectd.interface.if_dropped.tx	type: float **TODO**

collectd.virt フィールド
collectd 仮想プラグインに対応します。

collectd.virt.if_octets フィールド
collectd if_octets タイプの仮想プラグイン。

パラメーター	説明
collectd.virt.if_octets.rx	type: float **TODO**

パラメーター	説明
collectd.virt.if_octets.tx	type: float **TODO**

collectd.virt.if_packets フィールド
collectd if_packets タイプの仮想プラグイン。

パラメーター	説明
collectd.virt.if_packets.rx	type: float **TODO**
collectd.virt.if_packets.tx	type: float **TODO**

collectd.virt.if_errors フィールド
collectd if_errors タイプの仮想プラグイン。

パラメーター	説明
collectd.virt.if_errors.rx	type: float **TODO**
collectd.virt.if_errors.tx	type: float **TODO**

collectd.virt.if_dropped フィールド
collectd if_dropped タイプの仮想プラグイン。

パラメーター	説明
collectd.virt.if_dropped.rx	type: float **TODO**
collectd.virt.if_dropped.tx	type: float **TODO**

collectd.virt.disk_ops フィールド
collectd disk_ops タイプの仮想プラグイン。

パラメーター	説明
collectd.virt.disk_ops.read	type: float **TODO**
collectd.virt.disk_ops.write	type: float **TODO**

collectd.virt.disk_octets フィールド
collectd disk_octets タイプの仮想プラグイン。

パラメーター	説明
collectd.virt.disk_octets.read	type: float **TODO**
collectd.virt.disk_octets.write	type: float **TODO**
collectd.virt.memory	type: float **collectd** メモリータイプの仮想プラグイン。
collectd.virt.virt_vcpu	type: float **collectd virt_vcpu** タイプの仮想プラグイン。
collectd.virt.virt_cpu_total	type: float **collectd virt_cpu_total** タイプの仮想プラグイン。

collectd.CPU フィールド
collectd CPU プラグインに対応します。

パラメーター	説明
collectd.CPU.percent	type: float **collectd** percent タイプの CPU プラグイン。

collectd.df フィールド
collectd df プラグインに対応します。

パラメーター	説明
collectd.df.df_complex	type: float **collectd df_complex** タイプの **df** プラグイン。
collectd.df.percent_bytes	type: float **collectd percent_bytes** タイプの **df** プラグイン。

collectd.entropy フィールド
collectd エントロピープラグインに対応します。

パラメーター	説明
collectd.entropy.entropy	type: integer **collectd** エントロピータイプのエントロピー プラグイン。

collectd.memory フィールド
collectd メモリープラグインに対応します。

パラメーター	説明
collectd.memory.memory	type: float **collectd** メモリータイプのメモリープラグイン。
collectd.memory.percent	type: float **collectd** パーセントタイプのメモリープラグイン。

collectd.swap フィールド
collectd swap プラグインに対応します。

パラメーター	説明
collectd.swap.swap	type: integer **collectd** swap タイプの swap プラグイン。
collectd.swap.swap_io	type: integer **collectd swap_io** タイプの swap プラグイン。

collectd.load フィールド
collectd ロードプラグインに対応します。

collectd.load.load フィールド
collectd ロードタイプのロードプラグイン

パラメーター	説明
collectd.load.load.shortterm	type: float **TODO**
collectd.load.load.midterm	type: float **TODO**
collectd.load.load.longterm	type: float **TODO**

collectd.aggregation フィールド
collectd 集計プラグインに対応します。

パラメーター	説明
collectd.aggregation.percent	type: float **TODO**

collectd.statsd フィールド
collectd statsd プラグインに対応します。

パラメーター	説明
collectd.statsd.host_cpu	type: integer **collectd** CPU タイプの **statsd** プラグイン。
collectd.statsd.host_elapsed_time	type: integer **collectd elapsed_time** タイプの **statsd** プラグイン。
collectd.statsd.host_memory	type: integer **collectd** メモリータイプの **statsd** プラグイン。
collectd.statsd.host_nic_speed	type: integer **collectd nic_speed** タイプの **statsd** プラグイン。
collectd.statsd.host_nic_rx	type: integer **collectd nic_rx** タイプの **statsd** プラグイン。

パラメーター	説明
collectd.statsd.host_nic_tx	type: integer **collectd nic_tx** タイプの **statsd** プラグイン。
collectd.statsd.host_nic_rx_dropped	type: integer **collectd nic_rx_dropped** タイプの **statsd** プラグイン。
collectd.statsd.host_nic_tx_dropped	type: integer **collectd nic_tx_dropped** タイプの **statsd** プラグイン。
collectd.statsd.host_nic_rx_errors	type: integer **collectd nic_rx_errors** タイプの **statsd** プラグイン。
collectd.statsd.host_nic_tx_errors	type: integer **collectd nic_tx_errors** タイプの **statsd** プラグイン。
collectd.statsd.host_storage	type: integer **collectd** ストレージタイプの **statsd** プラグイン。
collectd.statsd.host_swap	type: integer **collectd** swap タイプの **statsd** プラグイン。
collectd.statsd.host_vdsm	type: integer **collectd** VDSM タイプの **statsd** プラグイン。
collectd.statsd.host_vms	type: integer **collectd** VMS タイプの**statsd** プラグイン。
collectd.statsd.vm_nic_tx_dropped	type: integer **collectd nic_tx_dropped** タイプの **statsd** プラグイン。
collectd.statsd.vm_nic_rx_bytes	type: integer **collectd nic_rx_bytes** タイプの **statsd** プラグイン。
collectd.statsd.vm_nic_tx_bytes	type: integer **collectd nic_tx_bytes** タイプの **statsd** プラグイン。

パラメーター	説明
collectd.statsd.vm_balloon_min	type: integer **collectd balloon_min** タイプの **statsd** プラグイン。
collectd.statsd.vm_balloon_max	type: integer **collectd balloon_max** タイプの **statsd** プラグイン。
collectd.statsd.vm_balloon_target	type: integer **collectd balloon_target** タイプの **statsd** プラグイン。
collectd.statsd.vm_balloon_cur	type: integer **collectd balloon_cur** タイプの **statsd** プラグイン。
collectd.statsd.vm_cpu_sys	type: integer **collectd cpu_sys** タイプの **statsd** プラグイン。
collectd.statsd.vm_cpu_usage	type: integer **collectd cpu_usage** タイプの **statsd** プラグイン。
collectd.statsd.vm_disk_read_ops	type: integer **collectd disk_read_ops** タイプの **statsd** プラグイン。
collectd.statsd.vm_disk_write_ops	type: integer **collectd disk_write_ops** タイプの **statsd** プラグイン。
collectd.statsd.vm_disk_flush_latency	type: integer **collectd disk_flush_latency** タイプの **statsd** プラグイン。
collectd.statsd.vm_disk_apparent_size	type: integer **collectd disk_apparent_size** タイプの **statsd** プラグイン。
collectd.statsd.vm_disk_write_bytes	type: integer **collectd disk_write_bytes** タイプの **statsd** プラグイン。
collectd.statsd.vm_disk_write_rate	type: integer **collectd disk_write_rate** タイプの **statsd** プラグイン。

パラメーター	説明
collectd.statsd.vm_disk_true_size	type: integer **collectd disk_true_size** タイプの **statsd** プラグイン。
collectd.statsd.vm_disk_read_rate	type: integer **collectd disk_read_rate** タイプの **statsd** プラグイン。
collectd.statsd.vm_disk_write_latency	type: integer **collectd disk_write_latency** タイプの **statsd** プラグイン。
collectd.statsd.vm_disk_read_latency	type: integer **collectd disk_read_latency** タイプの **statsd** プラグイン。
collectd.statsd.vm_disk_read_bytes	type: integer **collectd disk_read_bytes** タイプの **statsd** プラグイン。
collectd.statsd.vm_nic_rx_dropped	type: integer **collectd nic_rx_dropped** タイプの **statsd** プラグイン。
collectd.statsd.vm_cpu_user	type: integer **collectd cpu_user** タイプの **statsd** プラグイン。
collectd.statsd.vm_nic_rx_errors	type: integer **collectd nic_rx_errors** タイプの **statsd** プラグイン。
collectd.statsd.vm_nic_tx_errors	type: integer **collectd nic_tx_errors** タイプの **statsd** プラグイン。
collectd.statsd.vm_nic_speed	type: integer **collectd nic_speed** タイプの **statsd** プラグイン。

collectd.postgresql フィールド
collectd postgresql プラグインに対応します。

パラメーター	説明
collectd.postgresql.pg_n_tup_g	type: integer **collectd pg_n_tup_g** タイプの postgresql プラグイン。

パラメーター	説明
collectd.postgresql.pg_n_tup_c	type: integer **collectd pg_n_tup_c** タイプの postgresql プラグイン。
collectd.postgresql.pg_numbackends	type: integer **collectd pg_numbackends** タイプの postgresql プラグイン。
collectd.postgresql.pg_xact	type: integer **collectd pg_xact** タイプの postgresql プラグイン。
collectd.postgresql.pg_db_size	type: integer **collectd pg_db_size** タイプの postgresql プラグイン。
collectd.postgresql.pg_blks	type: integer **collectd pg_blks** タイプの postgresql プラグイン。

11.2. SYSTEMD のエクスポートされるフィールド

これらのフィールドは OpenShift Container Platform クラスターロギングによってエクスポートされる **systemd** フィールドであり、Elasticsearch および Kibana での検索に利用できます。

systemd ジャーナルに固有の共通フィールドが含まれます。アプリケーション は、独自のフィールドをジャーナルに書き込む可能性があります。それらは **systemd.u** namespace で利用できます。**RESULT** および **UNIT** はこれらの 2 つのフィールドです。

systemd.k フィールド
以下の表には、**systemd** カーネル固有のメタデータが含まれます。

パラメーター	説明
systemd.k.KERNEL_DEVICE	**systemd.k.KERNEL_DEVICE** は、カーネルのデバイス名です。
systemd.k.KERNEL_SUBSYSTEM	**systemd.k.KERNEL_SUBSYSTEM** は、カーネルのサブシステム名です。
systemd.k.UDEV_DEVLINK	**systemd.k.UDEV_DEVLINK** には、ノードを参照する追加のシンボリックリンク名が含まれます。
systemd.k.UDEV_DEVNODE	**systemd.k.UDEV_DEVNODE** は、デバイスのノードパスです。
systemd.k.UDEV_SYSNAME	**systemd.k.UDEV_SYSNAME** は、カーネルのデバイス名です。

パラメーター	説明

systemd.t フィールド
systemd.t Fields は信頼されたジャーナルフィールドであり、ジャーナルによって暗黙的に追加されるフィールドであり、クライアントノードで変更することはできません。

パラメーター	説明
systemd.t.AUDIT_LOGINUID	**systemd.t.AUDIT_LOGINUID** は、ジャーナルエントリープロセスのユーザー ID です。
systemd.t.BOOT_ID	**systemd.t.BOOT_ID** は、カーネルのブート ID です。
systemd.t.AUDIT_SESSION	**systemd.t.AUDIT_SESSION** は、ジャーナルエントリープロセスのセッションです。
systemd.t.CAP_EFFECTIVE	**systemd.t.CAP_EFFECTIVE** は、ジャーナルエントリープロセスの機能を表します。
systemd.t.CMDLINE	**systemd.t.CMDLINE** は、ジャーナルエントリープロセスのコマンドラインです。
systemd.t.COMM	**systemd.t.COMM** は、ジャーナルエントリープロセスの名前です。
systemd.t.EXE	**systemd.t.EXE** は、ジャーナルエントリープロセスの実行可能パスです。
systemd.t.GID	**systemd.t.GID** は、ジャーナルエントリープロセスのグループ ID です。
systemd.t.HOSTNAME	**systemd.t.HOSTNAME** は、ホストの名前です。
systemd.t.MACHINE_ID	**systemd.t.MACHINE_ID** は、ホストのマシン ID です。
systemd.t.PID	**systemd.t.PID** は、ジャーナルエントリープロセスのプロセス ID です。
systemd.t.SELINUX_CONTEXT	**systemd.t.SELINUX_CONTEXT** は、ジャーナルエントリープロセスのセキュリティーコンテキストまたはラベルです。
systemd.t.SOURCE_REALTIME_TIMESTAMP	**systemd.t.SOURCE_REALTIME_TIMESTAMP** は、最も早くかつ最も信頼できるメッセージのタイムスタンプです。これは RFC 3339 NS 形式に変換されます。
systemd.t.SYSTEMD_CGROUP	**systemd.t.SYSTEMD_CGROUP** は、**systemd** コントロールグループパスです。

パラメーター	説明
systemd.t.SYSTEMD_OWNER_UID	**systemd.t.SYSTEMD_OWNER_UID** は、セッションの所有者 ID です。
systemd.t.SYSTEMD_SESSION	**systemd.t.SYSTEMD_SESSION** は、(該当する場合) **systemd** セッション ID です。
systemd.t.SYSTEMD_SLICE	**systemd.t.SYSTEMD_SLICE** は、ジャーナルエントリープロセスのスライス (slice) ユニットです。
systemd.t.SYSTEMD_UNIT	**systemd.t.SYSTEMD_UNIT** は、セッションのユニット名です。
systemd.t.SYSTEMD_USER_UNIT	**systemd.t.SYSTEMD_USER_UNIT** は、(該当する場合) セッションのユーザーユニット名です。
systemd.t.TRANSPORT	**systemd.t.TRANSPORT** は、ジャーナルサービス別のエントリーのメソッドです。これには、**audit**、**driver**、**syslog**、**journal**、**stdout**、および **kernel** が含まれます。
systemd.t.UID	**systemd.t.UID** は、ジャーナルエントリープロセスのユーザー ID です。
systemd.t.SYSLOG_FACILITY	**systemd.t.SYSLOG_FACILITY** は、**syslog** の 10 進数の文字列としてフォーマットされる機能を含むフィールドです。
systemd.t.SYSLOG_IDENTIFIER	**systemd.t.systemd.t.SYSLOG_IDENTIFIER** は、**syslog** の識別子です。
systemd.t.SYSLOG_PID	**SYSLOG_PID** は、**syslog** のクライアントプロセス ID です。

systemd.u フィールド
systemd.u Fields はクライアントから直接渡され、ジャーナルに保存されます。

パラメーター	説明
systemd.u.CODE_FILE	**systemd.u.CODE_FILE** は、ソースのファイル名が含まれるコードの場所です。
systemd.u.CODE_FUNCTION	**systemd.u.CODE_FUNCTION** は、ソースの関数が含まれるコードの場所です。
systemd.u.CODE_LINE	**systemd.u.CODE_LINE** は、ソースの行数が含まれるコードの場所です。

パラメーター	説明
systemd.u.ERRNO	**systemd.u.ERRNO** は (ある場合)、10 進数の文字列として数値でフォーマットされる低位のエラー番号です。
systemd.u.MESSAGE_ID	**systemd.u.MESSAGE_ID** は、メッセージタイプを認識するためのメッセージ識別子の ID です。
systemd.u.RESULT	非公式の使用のみの場合に限定されます。
systemd.u.UNIT	非公式の使用のみの場合に限定されます。

11.3. KUBERNETES のエクスポートされるフィールド

これらは OpenShift Container Platform クラスターロギングでエクスポートされる Kubernetes フィールドであり、Elasticsearch および Kibana での検索に利用できます。

Kubernetes 固有メタデータの namespace です。**kubernetes.pod_name** は Pod の名前です。

kubernetes.labels フィールド
OpenShift オブジェクトに割り当てられるラベルは **kubernetes.labels** です。各ラベル名はラベルフィールドのサブフィールドです。それぞれのラベル名ではドットが取られます。つまり、名前のドットはアンダースコアに置き換えられます。

パラメーター	説明
kubernetes.pod_id	Pod の Kubernetes ID。
kubernetes.namespace_name	Kubernetes の namespace の名前。
kubernetes.namespace_id	Kubernetes の namespace の ID。
kubernetes.host	Kubernetes ノード名。
kubernetes.container_name	Kubernetes のコンテナーの名前。
kubernetes.labels.deployment	Kubernetes オブジェクトに関連付けられるデプロイメント。
kubernetes.labels.deploymentconfig	Kubernetes オブジェクトに関連付けられる deploymentconfig。
kubernetes.labels.component	Kubernetes オブジェクトに関連付けられるコンポーネント。

パラメーター	説明
kubernetes.labels.provider	Kubernetes オブジェクトに関連付けられるプロバイダー。

kubernetes.annotations フィールド
OpenShift オブジェクトに関連付けられるアノテーションは **kubernetes.annotations** フィールドです。

11.4. コンテナーのエクスポートされるフィールド

これらは OpenShift Container Platform クラスターロギングによってエクスポートされる Docker フィールドであり、Elasticsearch および Kibana での検索に利用できます。namespace は docker コンテナー固有のメタデータの namespace です。docker.container_id は Docker コンテナー ID です。

pipeline_metadata.collector フィールド
このセクションには、コレクターに固有のメタデータが含まれます。

パラメーター	説明
pipeline_metadata.collector.hostname	コレクターの FQDN。これはログの実際のエミッターの FQDN とは異なる場合があります。
pipeline_metadata.collector.name	コレクターの名前。
pipeline_metadata.collector.version	コレクターのバージョン。
pipeline_metadata.collector.ipaddr4	コレクターサーバーの IP アドレス v4。 配列である場合があります。
pipeline_metadata.collector.ipaddr6	コレクターサーバーの IP アドレス v6 。 配列である場合があります。
pipeline_metadata.collector.inputname	ログメッセージがコレクターによって受信された方法。TCP/UDP または imjournal/imfile。
pipeline_metadata.collector.received_at	メッセージがコレクターによって受信された時間。
pipeline_metadata.collector.original_raw_message	コレクターで収集された、解析されていない元のログメッセージ、または限りなくソースに近いログメッセージ。

pipeline_metadata.normalizer フィールド
このセクションには、ノーマライザーに固有のメタデータが含まれます。

パラメーター	説明
pipeline_metadata.normalizer.hostname	ノーマライザーの FQDN。
pipeline_metadata.normalizer.name	ノーマライザーの名前。
pipeline_metadata.normalizer.version	ノーマライザーのバージョン。
pipeline_metadata.normalizer.ipaddr4	ノーマライザーサーバーの IP アドレス v4。 配列である場合があります。
pipeline_metadata.normalizer.ipaddr6	ノーマライザーサーバーの IP アドレス v6 。配列である場合があります。
pipeline_metadata.normalizer.inputname	ログメッセージがノーマライザーによって受信された方法。TCP/UDP かどうか。
pipeline_metadata.normalizer.received_at	メッセージがノーマライザーによって受信された時間。
pipeline_metadata.normalizer.original_raw_message	ノーマライザーで受信される、解析されていない元のログメッセージ。
pipeline_metadata.trace	このフィールドは、メッセージの追跡を記録します。各コレクターおよびノーマライザーは自らについての情報およびメッセージが処理された日時についての情報を追加します。

11.5. OVIRT のエクスポートされるフィールド

これらは OpenShift Container Platform クラスターロギングでエクスポートされる oVirt フィールドであり、Elasticsearch および Kibana での検索に利用できます。

oVirt メタデータの namespace。

パラメーター	説明
ovirt.entity	データソース、ホスト、VMS、およびエンジンのタイプ。
ovirt.host_id	oVirt ホストの UUID。

ovirt.engine フィールド
oVirt エンジン関連のメタデータの namespace。oVirt エンジンの FQDN は **ovirt.engine.fqdn** です。

11.6. AUSHAPE のエクスポートされるフィールド

これらは OpenShift Container Platform クラスターロギングでエクスポートされる Aushape フィールドであり、Elasticsearch および Kibana での検索に利用できます。

Aushape で変換される監査イベント。詳細は Aushape を参照してください。

パラメーター	説明
aushape.serial	監査イベントのシリアル番号。
aushape.node	監査イベントが発生したホストの名前。
aushape.error	イベントの変換中に aushape に発生したエラー。
aushape.trimmed	イベントオブジェクトに関連する JSONPath 表現の配列であり、イベントサイズの制限の結果として削除されたコンテンツを持つオブジェクトまたは配列を指定します。空の文字列は、イベントがコンテンツを削除したことを意味し、空の配列は、指定されていないオブジェクトおよび配列によってトリミングが生じたことを意味します。
aushape.text	元の監査イベントを表す配列ログレコード文字列。

aushape.data フィールド
Aushape に関連する解析された監査イベントデータ。

パラメーター	説明
aushape.data.avc	type: nested
aushape.data.execve	type: string
aushape.data.netfilter_cfg	type: nested
aushape.data.obj_pid	type: nested
aushape.data.path	type: nested

11.7. TLOG のエクスポートされるフィールド

これらは OpenShift Container Platform クラスターロギングでエクスポートされる Tlog フィールドであり、Elasticsearch および Kibana での検索に利用できます。

Tlog ターミナル I/O の記録メッセージ。詳細は Tlog を参照してください。

パラメーター	説明
tlog.ver	メッセージ形式のバージョン番号。

パラメーター	説明
tlog.user	記録されたユーザー名。
tlog.term	ターミナルタイプ名。
tlog.session	記録されたセッションの監査セッション ID。
tlog.id	セッション内のメッセージの ID。
tlog.pos	セッション内のメッセージの位置 (ミリ秒単位)。
tlog.timing	このメッセージのイベントの配分 (時間)。
tlog.in_txt	無効な文字が除去された入力テキスト。
tlog.in_bin	除去された無効な入力文字 (バイト)。
tlog.out_txt	無効な文字が除去された出力テキスト。
tlog.out_bin	除去された無効な出力文字 (バイト)。