

# NEC Workload Manager for Container Platform Manual SystemManager G 連携

本書では、NEC Workload Manager for Container Platform と WebSAM SystemManager G との連携手順について説明します。

## 連携イメージ

- SystemManager G で Kubernetes コンテナのアプリケーション障害を検知し、Workload Manager の情報採取コマンド実行します。
- Kubernetes コンテナのアプリケーションは、stdout/stderr にログを書き込む作法となっています。これらのログは、fluentd が収集して外部サーバにログファイルに送信することができる。この外部サーバに集約されたログファイルを SystemManager G アプリケーションログ監視機能で監視し、障害を検知したらアクション実行で Workload Manager のコマンド実行します。

(注意事項) 従来のサーバからの Lift でアプリケーションが個別のファイルに書き込む方式の場合は本方法は使えません。

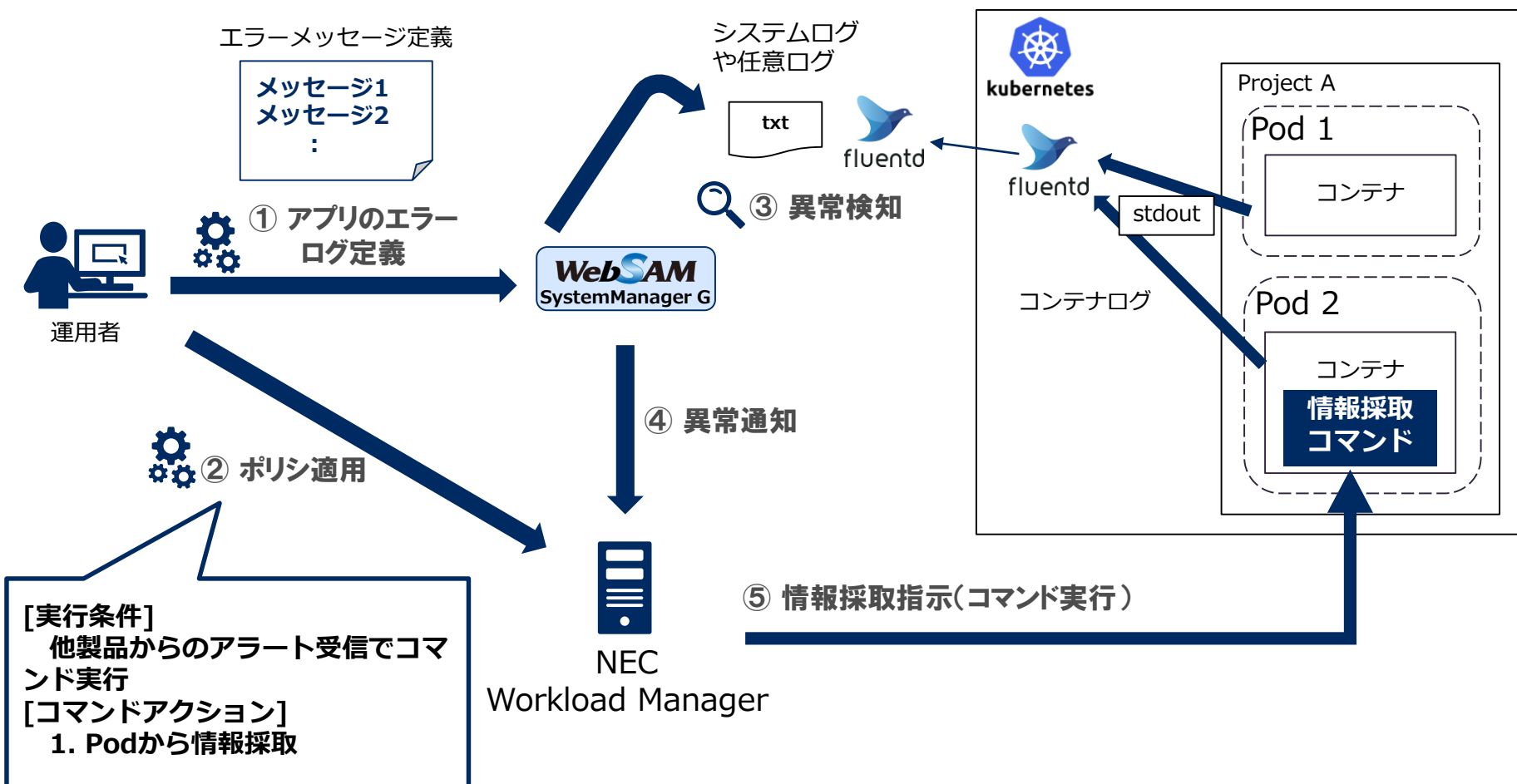
以降の手順は、以下の作業が完了し、SystemManager G が Kubernetes コンテナのアプリケーションログを監視できる状態になっている事を前提としています。

- fluentd のインストール
- fluentd を用いて、Kubernetes コンテナのアプリケーションログをログサーバへ転送する設定

本書の付録に、参考として上記の手順を記載しております。

# SystemManager G 連携イメージ

SystemManager G でコンテナアプリケーションのログ監視を行い、アプリケーションエラー時に Workload Manager で Pod の情報採取



- NEC Workload Manager for Container Platform の動作環境に準拠します。
- 連携対象の SystemManager G の対応バージョン
  - WebSAM SystemManager G 9.0.0

## 手順の流れ

### - SystemManager G の設定 -

1. 概要
2. fluentd が収集したログを監視設定する
3. フィルタ設定のフィルタ定義で検知したいメッセージのフィルタ設定する
4. フィルタ設定の表示定義でノードをPod 名に置換する設定をする
5. カテゴリを作成する
6. フィルタ設定のフィルタ定義でアプリケーションログのフィルタ設定
7. フィルタ設定のリカバリ定義でアクション通報を行う。ここで Workload Manager のコマンドを設定する。

### - Workload Manager の設定 -

1. ログイン
2. ポリシー追加

## アプリケーションログ監視機能の設定

1. 外部サーバにある fluentd が収集したログを監視対象として設定する。
2. フィルタ設定のフィルタ定義で検知したいメッセージのフィルタ設定する。
3. フィルタ設定の表示定義でノードを Pod 名 + ネームスペースに置換する設定をする。

## ビジネスビュー機能の設定

4. カテゴリを作成する。
5. フィルタ設定のフィルタ定義でアプリケーションログのフィルタ設定をする。
6. フィルタ設定のリカバリ定義でアクション通報を行う。ここで Workload Manager のコマンドを設定する。

## 補足

- ノード名を変えてしまうのでメッセージ監視にはメッセージが格納されない。よって、ビジネスビューでメッセージ格納とアクション通報を行う。

# fluentd が収集したログを監視設定する

サーバの fluentd が収集したログの監視設定をする。ローテーションする場合はバックアップファイルにも監視設定が必要。

fluentd で収集した Kubernetes コンテナのアプリケーションログのファイルパスを指定して下さい。

WebSAM Integrated Console - [トポロジビュー - rhel75 - アプリケーションログ監視 - messages]

ファイル(F) 表示(V) 操作(O) 設定(S) ウィンドウ(W) ヘルプ(H)

システム

- トポロジビュー
  - WIN-KQOLAEHACMT
    - アプリケーションログ監視
      - messages
      - システム
      - システムログ監視
      - メッセージ監視
      - 性能監視
      - 未登録のホスト
- ビジネスビュー
  - fluentd
  - Unified Management Framework
  - アプリケーションビュー
  - イベントコリレーションビュー
  - オーデイトログ
  - メッセージ連携
  - マルチグラフビュー
  - 印刷ビュー
  - アプリケーション管理ビュー

アプリケーションログ監視設定

messages

親グループ: アプリケーションログ監視

アプリケーションログ名(N): messages

アイコンファイル(I):

ログファイル名(L): /var/log/messages 参照...

バックアップファイル

監視する(B)

No.	ログファイル名
-----	---------

↑ (P) ↓ (O) 編集(U) 追加(A) 削除(D)

文字コード(C): US-ASCII オプション(Z)

OK キャンセル

通報状態	通報日	通報時刻	サービス
正常終了	2019/05/28	19:16:51	BusinessService
正常終了	2019/05/28	19:21:11	BusinessService
正常終了	2019/06/03	09:24:01	BusinessService
正常終了	2019/06/03	11:00:11	BusinessService
正常終了	2019/06/03	11:00:11	BusinessService

# フィルタ設定のフィルタ定義で検知したいメッセージのフィルタ設定する

WebSAM Integrated Console - [トポロジビュー - rhel75 - アプリケーションログ監視 - messages]

ファイル(F) 表示(V) 操作(O) 設定(S) ウィンドウ(W) ヘルプ(H)

システム

トポロジビュー

- WIN-KQOLAEHACMT
  - アプリケーションログ監視
    - messages
    - フィルタ定義
  - システム
  - シスログ監視
  - メッセージ監視
  - 性能監視
- 未登録のホスト
- ビジネスビュー
  - fluentd
  - Unified Management
  - アプリケーションビュー
  - イベントコリレーションビュー
  - オーデイトログ
  - メッセージ連携
  - マルチグラフビュー
  - 印刷ビュー
  - アプリケーション管理ビュー

マップビュー プロパティビュー

messages

項目名	内容
error	

フィルタ定義

フィルタ名	タイプ	カテゴリ	重要度	ノード
error	追加	Application	異常	\$REXP("pod...

フィルタ項目設定

フィルタ定義 表示定義 オプション定義

メッセージ概要(D): error

タイプ(T):  格納  削除

メッセージテキスト(M): 否定  error

位置指定(P): No1 No2 No3 No4 No5 No6 No7 No8  
否定  位置: 1 条件: = 比較値:

キー指定(K): No1 No2 No3 No4 No5 No6 No7 No8  
否定  キー値: 条件: = 比較値:

OK キャンセル ヘルプ

通報状態	通報日	通報時刻	サービス名	概要
正常終了	2019/06/03	11:00:11	BusinessService	action
正常終了	2019/06/03	11:01:11	BusinessService	action
正常終了	2019/06/03	11:01:11	BusinessService	action
正常終了	2019/06/03	11:10:11	BusinessService	action
正常終了	2019/06/03	11:10:11	BusinessService	action



# フィルタ設定の表示定義でノードをPod名に置換する設定をする

WebSAM Integrated Console - [トボロジビュー - rhel75 - アプリケーションログ監視 - messages]

ファイル(F) 表示(V) 操作(O) 設定(S) ウィンドウ(W) ヘルプ(H)

システム

トボロジビュー

WIN-KQOLAEHACMT

アプリケーションログ監視

messages

システム

シスログ監視

メッセージ監視

性能監視

未登録のホスト

ビジネスビュー

fluentd

Unified Manager

アプリケーションビュー

イベントコリレーションビュー

オーデイトログ

メッセージ連携

マルチグラフビュー

印刷ビュー

アプリケーション管理ビュー

マップビュー プロパティビュー

messages

項目名 内容

タイプ アプリケーションログノード

フィルタ定義

フィルタ名	タイプ	カテゴリ	重要度	ノード
error	追加	Application	異常	\$REPEXP("pod_...

フィルタ項目設定

フィルタ定義 **表示定義** アプリケーション定義

重要度(S): 異常

カテゴリ(C): Application

ノード(N): \$REPEXP("pod\_name:.:.",".:.")

アプリケーション(A): \$REPEXP("mespace\_name:.:.",".:.")

オブジェクト(O): ApLogMonitor

メッセージID(I): 0000

OK キャンセル ヘルプ

通報状態	通報日	通報時刻	サービス	操作
正常終了	2019/06/03	11:20:11	BusinessService	action
正常終了	2019/06/03	11:20:11	BusinessService	action
正常終了	2019/06/03	11:30:11	BusinessService	action
正常終了	2019/06/03	11:30:12	BusinessService	action
正常終了	2019/06/03	11:37:21	BusinessService	action

ノードとアプリケーションに下記を設定する。

ノード:  
\$REPEXP("pod\_name:.:.",".:.")

アプリケーション:  
\$REPEXP("mespace\_name:.:.",".:.")

# カテゴリを作成する

WebSAM Integrated Console - [ビジネスビュー - fluentd]

ファイル(F) 表示(V) 操作(O) 設定(S) ウィンドウ(W) ヘルプ(H)

システム

マップビュー プロパティビュー

トポロジビュー

- WIN-KQOLAEHACMT
  - アプリケーションログ監視
    - messages
    - システム
    - シスログ監視
    - メッセージ監視
    - 性能監視
  - 未登録のホスト
- ビジネスビュー
  - fluentd**
  - Unified Management Framework
- アプリケーションビュー
- イベントコリレーションビュー
- オーディットログ
- メッセージ連携
- マルチグラフビュー
- 印刷ビュー
- アプリケーション管理ビュー

例: fluentd

項目名 内容

オーディットログ一覧 | メッセージ | オンラインメッセージ | リカバリステータス | 通報ステータス | イベントコリレーション

詳細表示... 検索... 確認 保存 スワップ... 初期化...

通報状態	通報日	通報時刻	サービス名	概要
正常終了	2019/06/03	11:10:11	BusinessService	action
正常終了	2019/06/03	11:20:11	BusinessService	action
正常終了	2019/06/03	11:20:11	BusinessService	action
正常終了	2019/06/03	11:30:11	BusinessService	action
正常終了	2019/06/03	11:30:12	BusinessService	action

# フィルタ設定のフィルタ定義でアプリケーションログのフィルタ設定をする

アプリケーションログのメッセージをフィルタする設定を行う

フィルタ項目設定

フィルタ定義 表示定義 リカバリ定義 オプション定義

メッセージ概要(D): action

タイプ(T):  格納  削除

カテゴリ(C): 否定  Application

ノード(N): 否定

アプリケーション(A): 否定

オブジェクト(O): 否定  ApLogMonitor

メッセージID(I): 否定  0000

メッセージテキスト(M): 否定

位置指定(P): No1 No2 No3 No4 No5 No6 No7 No8  
否定  位置: 1 条件: = 比較値:

キー指定(K): No1 No2 No3 No4 No5 No6 No7 No8  
否定  キー値: 条件: = 比較値:

重要度(S): 否定

OK キャンセル ヘルプ

通報状態	通報日	通報時刻	サービス名
正常終了	2019/06/03	11:30:11	BusinessService
正常終了	2019/06/03	11:30:12	BusinessService
正常終了	2019/06/03	11:37:21	BusinessService
正常終了	2019/06/03	11:40:11	BusinessService
正常終了	2019/06/03	11:40:11	BusinessService

Workload Manager の下記のコマンドを媒体からコピーし、SystemManager G がインストールされたマシンの任意の場所に配置して下さい。

- Windowsの場合
  - command¥windows¥fire\_wm\_policy.cmd
  - command¥windows¥fire\_wm\_policy.ps1
- Linuxの場合
  - command¥linux¥fire\_wm\_policy.sh

## コマンドファイルの修正

- WM\_URL に「Workload Manager の URL」を設定してください。
  - Windowsの場合 : fire\_wm\_policy.ps1

```
# Must *CHANGE* WM_URL
$WM_URL = "https://"

:(中略)
```

- Linuxの場合 : fire\_wm\_policy.sh

```
# MUST *CHANGE* WM_URL
WM_URL="https://"

:(中略)
```

# フィルタ設定のリカバリ定義でアクション通報を行う。ここで Workload Manager のコマンドを設定する。(2/2)

アクション通報で Workload Managerのコマンドを設定する。  
P12のコマンドを設定してください。

コマンド : `fire_wm_policy.cmd`  
オプション : `ポリシーID $APPLICATION$ $NODE$`

ポリシーID: アクション発動対象のポリシーのID  
\$APPLICATION: Podネームスペース  
\$NODE: Pod名

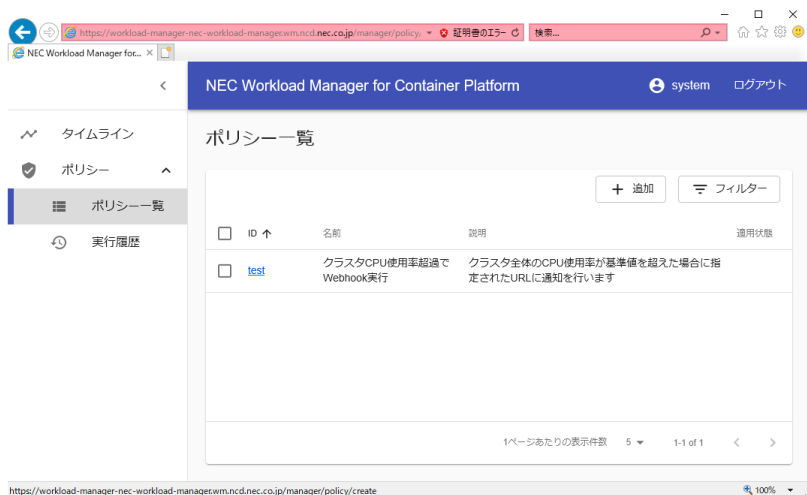
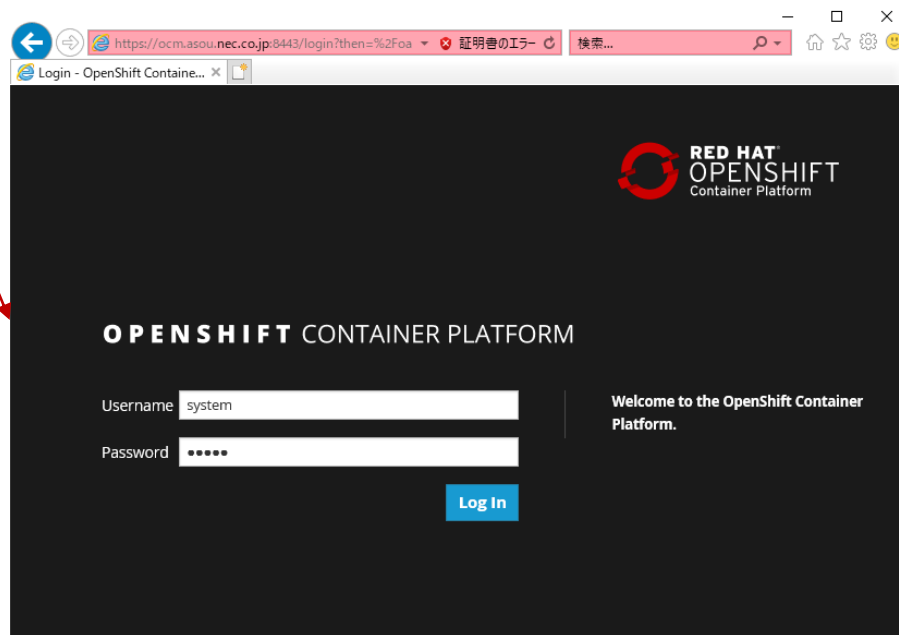
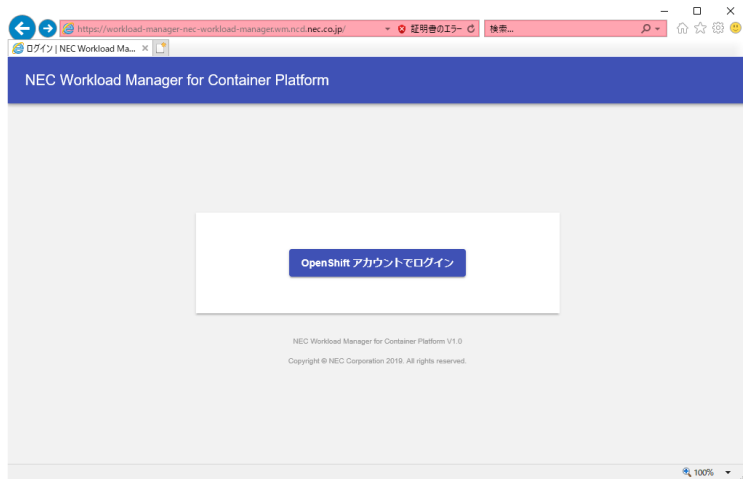
The screenshot shows the WebSAM Integrated Console interface. The 'フィルタ項目設定' (Filter Item Settings) dialog is open, with the 'リカバリ定義' (Recovery Definition) tab selected. The '通知指定(E):' (Notification Specification) checkbox is checked, and the '通知設定...' (Notification Settings...) button is highlighted with a red arrow. The '通知設定' (Notification Settings) dialog is also open, showing the 'アクション通報' (Action Notification) tab. The 'アクション通報を行う(E):' (Perform Action Notification) checkbox is checked. The 'ポリシー名(P):' (Policy Name) dropdown is set to 'Workload Manager'. The 'コマンド:' (Command) field contains 'C:\wm\fire\_wm\_policy.cmd'. The 'オプション:' (Options) field contains 'sysmer01 \$APPLICATION\$ \$NODE\$'. The '通知設定' dialog has 'OK', 'キャンセル', and 'ヘルプ' buttons.

フィルタ名	タイプ	カテゴリ
action	追加	App

通報状態	通報日	通報時刻	サービス名	概要
正常終了	2019/06/03	16:00:11	BusinessService	action
正常終了	2019/06/03	16:01:11	BusinessService	action
正常終了	2019/06/03	16:01:11	BusinessService	action
正常終了	2019/06/03	16:10:11	BusinessService	action
正常終了	2019/06/03	16:10:12	BusinessService	action

# Workload Manager へログイン

OpenShift のログイン画面からログイン → ポリシー一覧画面を選択



# ポリシー追加 (1/2)

ポリシー追加画面から「別製品からのアラート受信で..」を選択

The screenshot displays the NEC Workload Manager for Container Platform web interface. The browser address bar shows the URL: <https://workload-manager-nec-workload-manager.wm.ncd.nec.co.jp/manager/policy/>. The page title is "NEC Workload Manager for Container Platform". The user is logged in as "system" and can click "ログアウト".

The left sidebar contains the following menu items:

- タイムライン
- ポリシー
- ポリシー一覧 (highlighted)
- 実行履歴

The main content area shows a dropdown menu with the following options:

- クラスタCPU使用率超過でPod再スケジュール
- クラスタCPU使用率超過でWebhook実行
- クラスタメモリ使用率超過でPod再スケジュール
- クラスタメモリ使用率超過でWebhook実行
- 別製品からのアラート受信でコマンド実行
- 別製品からのアラート受信でPod再スケジュール
- 別製品からのアラート受信でWebhook実行
- ノードCPU使用率超過でPod再スケジュール
- ノードCPU使用率超過でWebhook実行
- ノード停止でWebhook実行

A blue "選択" (Select) button is positioned to the right of the dropdown menu. The browser status bar at the bottom indicates a zoom level of 100%.



# ポリシー追加 (2/2)

ポリシーのID には P13 の「ポリシーID」を指定して下さい。

The screenshot displays the 'Policy Addition' interface in the NEC Workload Manager. The browser address bar shows the URL: <https://workload-manager-nec-workload-manager.wm.ncd.nec.co.jp/manager/policy>. The page title is 'NEC Workload Manager for Container Platform'. The user is logged in as 'system' and can click 'ログアウト'. The left sidebar contains navigation options: 'タイムライン', 'ポリシー', 'ポリシー一覧', and '実行履歴'. The main content area is titled 'ポリシー追加' and contains the following form fields:

- 利用テンプレート:** A dropdown menu with the selected option '別製品からのアラート受信でコマンド実行' and a blue '選択' button.
- ID\*:** A text input field containing 'sysmgr01'. Below it, a note states: '1~256文字で入力してください。入力可能な文字は、英字・数字です。'
- 名前:** A text input field containing '別製品からのアラート受信でコマンド実行'. Below it, a note states: '1~1024文字で入力してください。'
- 説明:** A text input field containing '別製品からアラートを受信した場合に指定されたコマンドを実行します'. Below it, a note states: '1~1024文字で入力してください。'
- 監視間隔\*:** A partially visible field at the bottom.

The browser's status bar at the bottom shows the URL <https://workload-manager-nec-workload-manager.wm.ncd.nec.co.jp/manager/policy/create> and a zoom level of 100%.



## 付録：fluentd の設定

- fluentd のインストール
- fluentd を用いて、Kubernetes コンテナのアプリケーションログをログサーバへ転送する設定
- ログ転送設定の確認

## Kubernetes(OpenShift) ノード

- OpenShift の下記のマニュアルの「Deploying the EFK Stack」を参考にインストールしてください。インベントリファイルには下記のような内容を指定して下さい（下記の例は、PVにNFSを利用する例）。

- [https://docs.openshift.com/container-platform/3.11/install\\_config/aggregate\\_logging.html](https://docs.openshift.com/container-platform/3.11/install_config/aggregate_logging.html)

~/etc/ansible/hosts

```
[OSEv3:vars]
openshift_logging_install_logging=true
openshift_logging_es_memory_limit=8Gi
openshift_logging_storage_kind=nfs
openshift_logging_storage_access_modes=['ReadWriteOnce']
openshift_logging_storage_nfs_directory=NFSディレクトリ(環境に合わせて変更)
openshift_logging_storage_nfs_options='*(rw,root_squash)'
openshift_logging_storage_volume_name=logging
openshift_logging_storage_volume_size=10Gi
openshift_logging_storage_labels={'storage': 'logging'}
openshift_logging_es_nodeselector={'node-role.kubernetes.io/infra':'true'}
openshift_enable_unsupported_configurations=true
```

## System Manager G インストールノード

- 下記サイトからダウンロードし、インストールして下さい。

- <https://www.fluentd.org/download>

# ログ転送設定 (Kubernetes ノード側)

■ ネームスペース「openshift-logging」, ConfigMap「logging-fluentd」を編集する。変更後、fluentd の Pod (fluentd-xxx) を再起動します。

- fluentd の Pod の稼働状況確認

```
# oc get pod -n openshift-logging
```

NAME	READY	STATUS	RESTARTS	AGE
logging-curator-1560969000-8fjxr	0/1	Completed	0	6h
logging-es-data-master-sgeqpk40-2-5dd87	2/2	Running	0	18h
logging-fluentd-m69jp	1/1	Running	0	16h
logging-fluentd-qdccb	1/1	Running	0	16h
logging-fluentd-rbnjk	1/1	Running	0	16h
logging-kibana-1-g2ngm	2/2	Running	0	18h

- configMap を編集 (赤字のように編集)

```
# oc edit configmap/logging-fluentd -n openshift-logging
```

```
:
secure-forward.conf: |
  @type forward
  <server>
  host ログサーバのホスト名(IPアドレス)
  port 24224
  </server>
throttle-config.yaml: |
:
```

- fluentd の Pod を再起動

```
# oc delete pod $(oc get pod -n openshift-logging | grep fluentd | cut -d ' ' -f 1)
```

# ログ転送設定 (ログサーバ側)

[fluentdフォルダ]¥etc¥td-agent¥td-agent.conf。

- td-agent.conf に下記を追加

```
⋮
⋮
<match output_tag>
# @type stdout
# @id output_stdout
  @type file
# format single_value
  append true
  path /var/log/messages      # ログファイルパス : Kubernetes から収集したログファイル
<buffer>
  @type file
  path /var/log/fluentd/out
  flush_mode interval
  flush_interval 60s
</buffer>
</match>
⋮
⋮
```

- td-agent を起動

```
[fluentdフォルダ]¥embedded¥bin¥fluentd.bat -c [fluentdフォルダ]¥etc¥td-agent¥td-agent.conf
```

例

```
C:¥opt¥td-agent¥embedded¥bin¥fluentd.bat -c C:¥opt¥td-agent¥etc¥td-agent¥td-agent.conf
```

# ログ転送の確認

fluentd のログ転送が正常に動作しているか確認してください。

- SystemManager G のインストール先が Windows の場合

下記のログファイルが生成され、ファイル内にログメッセージが含まれていることを確認して下さい。

- C:¥var¥log 配下に messages.YYYYMMDD.log(例:messages.20190605.log)
- C:¥var¥log¥fluentd¥out フォルダ配下に中間ファイル

- SystemManager G のインストール先が Linux の場合

- /var/log/ 配下に messages.YYYYMMDD.log(例:messages.20190605.log)

C:¥var¥log¥messages.YYYYMMDD.log (/var/log/messages.YYYYMMDD.log) の例

```
2019-07-18T14:10:34+09:00      output_tag {"type":"log","@timestamp":"2019-07-18T05:10:34.8413441Z","tags":["warning","elasticsearch","admin"],"message":"Unable to revive connection: https://logging-es:9200/","docker":{"container_id":"27ab4deec3b198322f421748a912a94a690b73dee8e32769cd4e6abd1d0f4a43"},"kubernetes":{"container_name":"kibana","namespace_name":"openshift-logging","pod_name":"logging-kibana-1-g2ngm","pod_id":"81a55531-9258-11e9-8f7d-00155d2a9425","labels":{"component":"kibana","deployment":"logging-kibana-1","deploymentconfig":"logging-kibana"},"logging-infra":"kibana","provider":"openshift"},"host":"ocm.asou.nec.co.jp","master_url":"https://kubernetes.default.svc.cluster.local","namespace_id":" ...
```

ログ転送が出来ていない場合、ログサーバ(SystemManager G インストールホスト)と Kubernetes(OpenShift)ノード間でポート番号「24224」の通信が可能かどうか、Firewallの設定を確認して下さい。