IBM SevOne NPM NPM 設定ガイド
4. イベント監視

2022年6月10日
日本アイ・ビー・エム株式会社
データ・AI・オートメーション事業部

はじめに

■ 当資料の位置づけ

– 当資料は、IBM SevOne Network Performance Management (NPM) ソリューションのうち、Data Appliance NMS (PAS) とData Insightの構成およびこれらを使用した基本的な監視機能についての動作確認結果を設定ガイドとしてまとめたものです。SevOneの全機能、もしくはそれらの組み合わせを網羅した資料ではありません。

■ 注意事項

– 当資料に含まれる情報は可能な限り正確を期しておりますが、正式なレビューを受けておらず、当資料に記載された内容に関して何ら保証するものではありません。ここでの記載内容はあくまでも支援情報であり、使用者の責任において取扱われるものとし、資料の内容によって受けたいかなる損害に関して一切の保証をするものではありません。

■ 変更履歴

– 2022年4月　　初版 (v1.0) 作成
– 2022年5月　　juniper機器の検証結果を追記

※NMS: Network Management System
※PAS: Performance Appliance System

4. イベント監視

目次

4.1. Policy Browser

Policy Browser概要

- Policyは、しきい値など特定条件を満たした場合に、アラートやトラップなどをトリガーして通知する機能
- Device Group (もしくは Object Group) 単位でPolicyを適用可能
- Policy BrowserにてPolicyの作成・削除などの管理をする
- トリガー条件およびクリア条件を満たした際に以下の方法で通知可能
  - Email
  - SNMP Trap
  - Webhook

検証内容

- IP SLAのicmp-echoを監視するPolicyを作成、トリガー条件およびクリア条件を満たした際にアラートが通知されることを確認する
  - トリガー条件、クリア条件を満たすよう遅延装置 (WANem) にて遅延を設定・解除する
- 以下の各通知方法でどのように通知されるかを確認する
  - Email
  - Webhook

(参考) PolicyとThreshold

- PolicyとThresholdはどちらも指定した条件を満たした際にアラートやトラップなどをトリガーして通知する機能だが、条件の適用範囲が異なる
  - Threshold: 単一のデバイスに適用するトリガー条件およびクリア条件を定義可能
  - Policy: 複数デバイス (Device GroupまたはObject) に適用するトリガー条件およびクリア条件を定義可能

- Thresholdの制限として、通知先にWebhookを構成できない
  - 以下、マニュアル抜粋

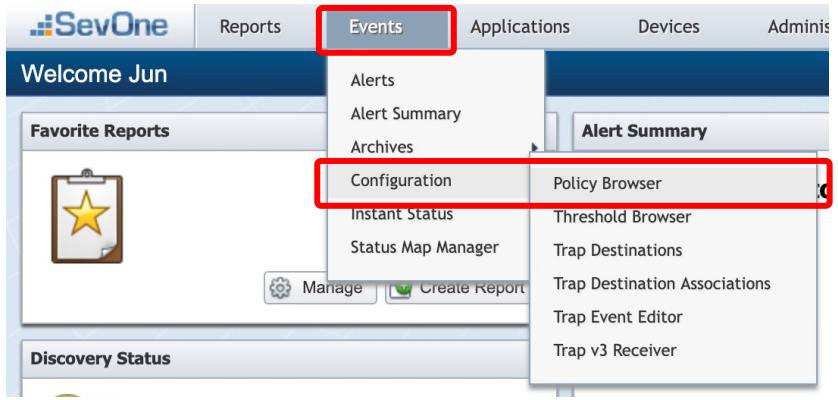
> ⛔ At present, Webhooks can only be configured on **Policies**. When adding **Thresholds**, although Webhooks are visible, they are **disabled** and cannot be configured.

4.1.1. 設定

1. Policyの作成
2. Email通知設定
3. Webhook通知設定

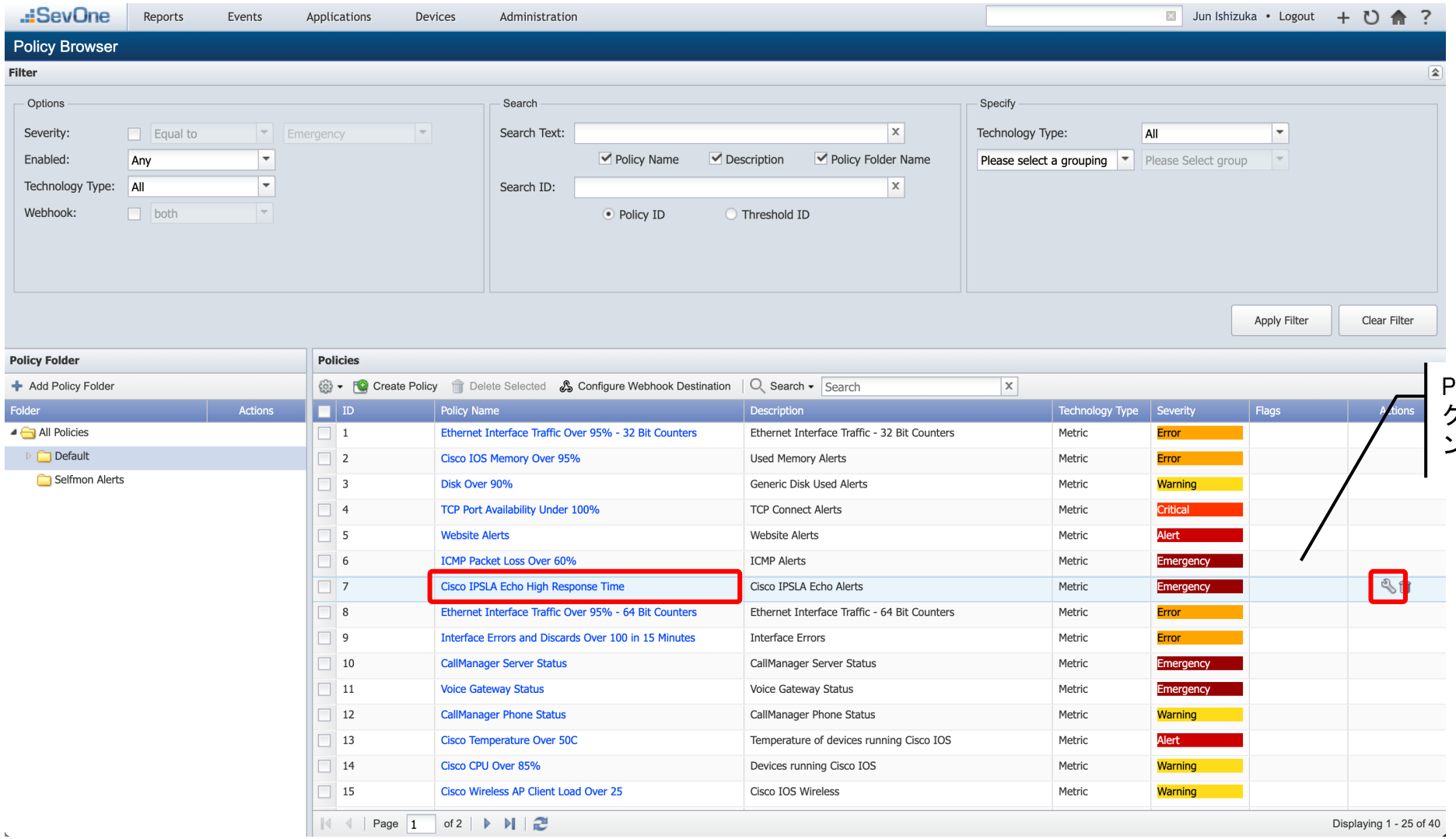
4.1.1.1. Policyの作成 (1/5)

■ メニュー・バーより、[Events] > [Configuration] > [Policy Browser] を選択



4.1.1.1. Policyの作成 (2/5)

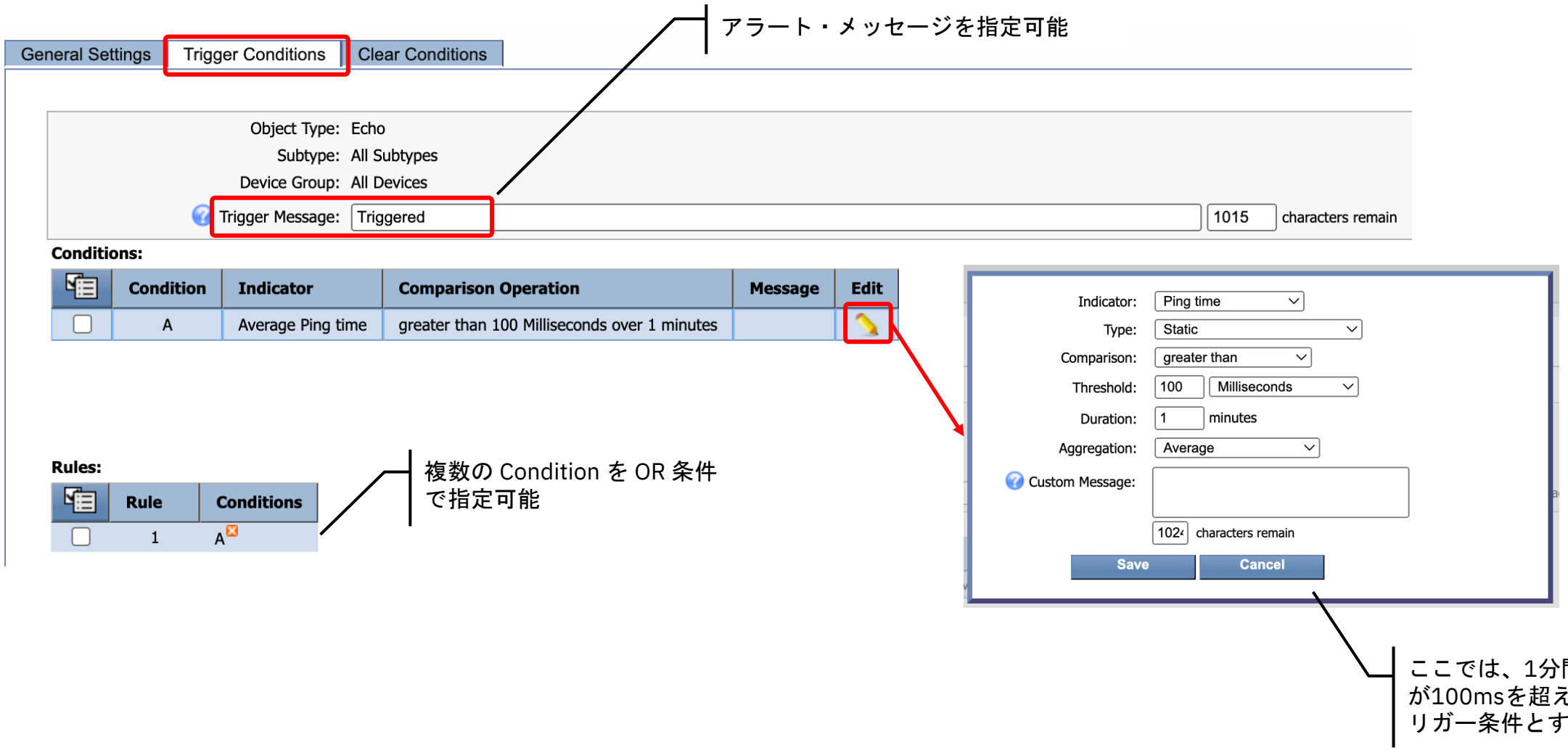
- ここでは、デフォルトで提供されるPolicyをカスタマイズして使用するため、IP SLA用のPolicyを選択



Policy Nameのリンクをクリックするか、右端の [Edit] アイコンをクリックする

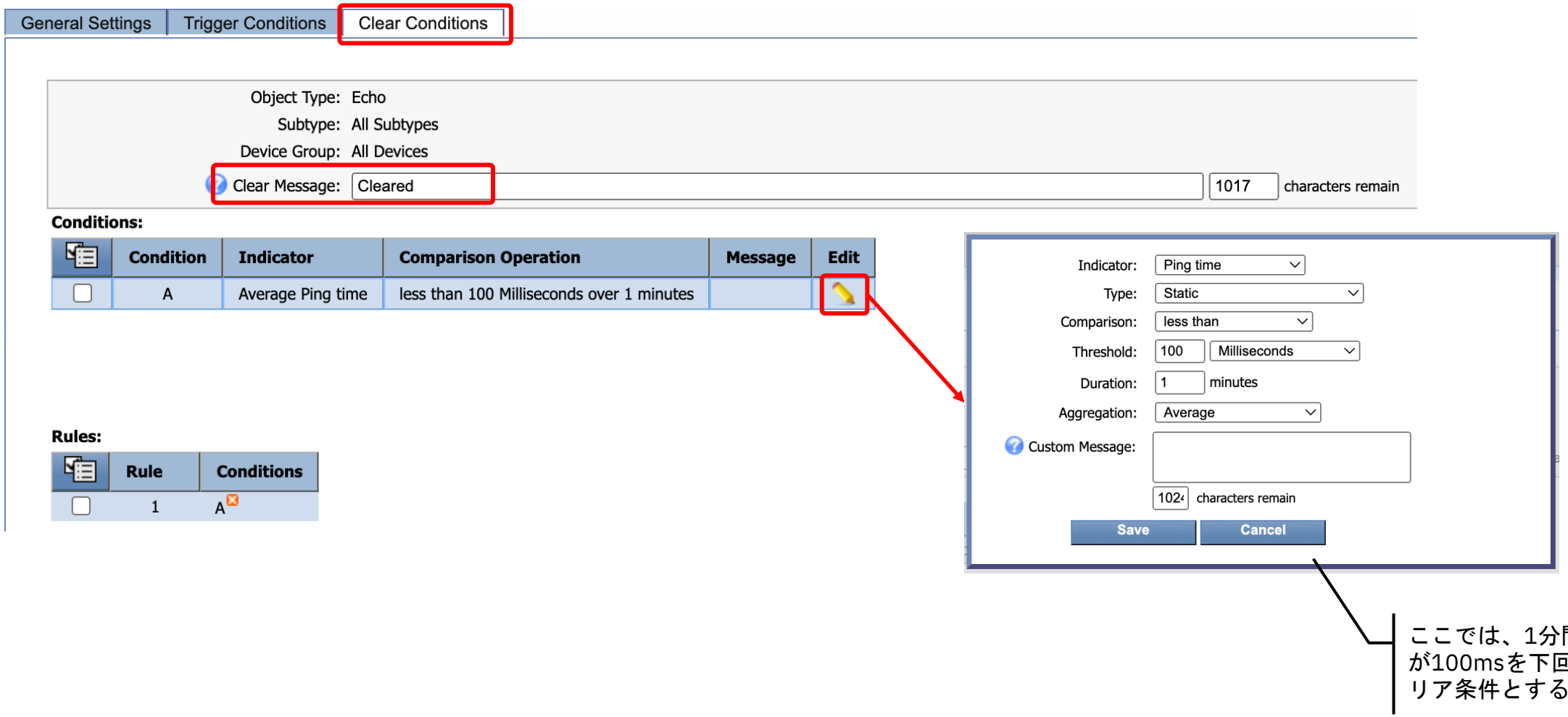
4.1.1.1. Policyの作成 (3/5)

■ [Trigger Conditions] タブを開き、トリガー条件を編集する



4.1.1.1. Policyの作成 (4/5)

- [Clear Conditions] タブを開き、同様に編集する

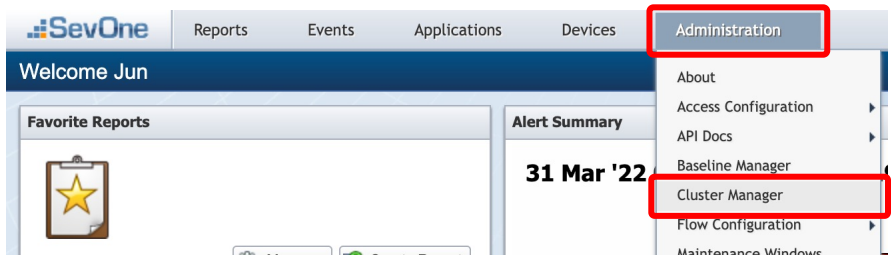


4.1.1.1. Policyの作成 (5/5)

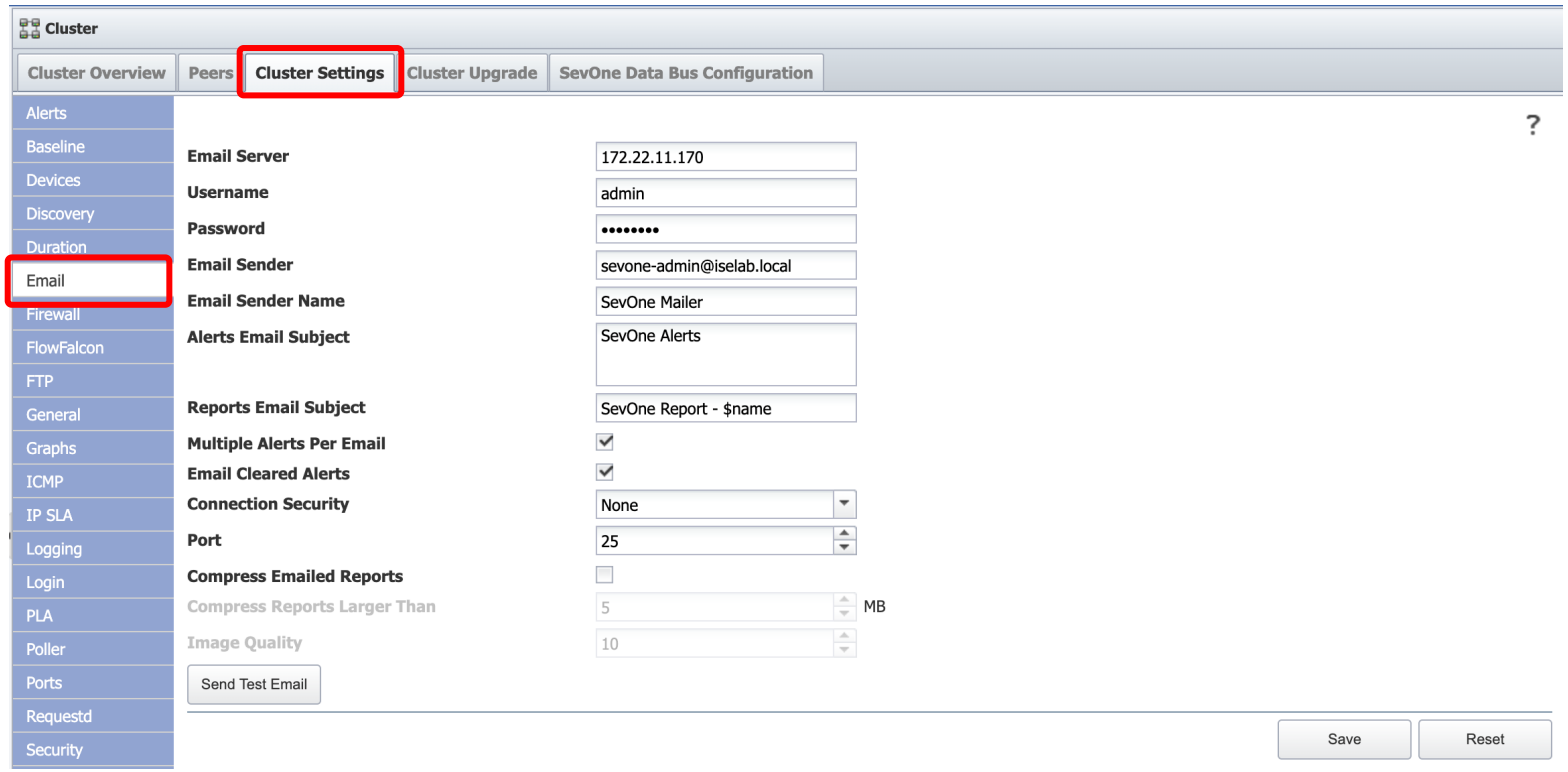
- [General Settings] を開き、任意の名前を指定して [Save as New] ボタン押下で新規ポリシーとして保存

4.1.1.2. Email通知設定 (1/2)

- [Administration] > [Cluster Manager] を選択

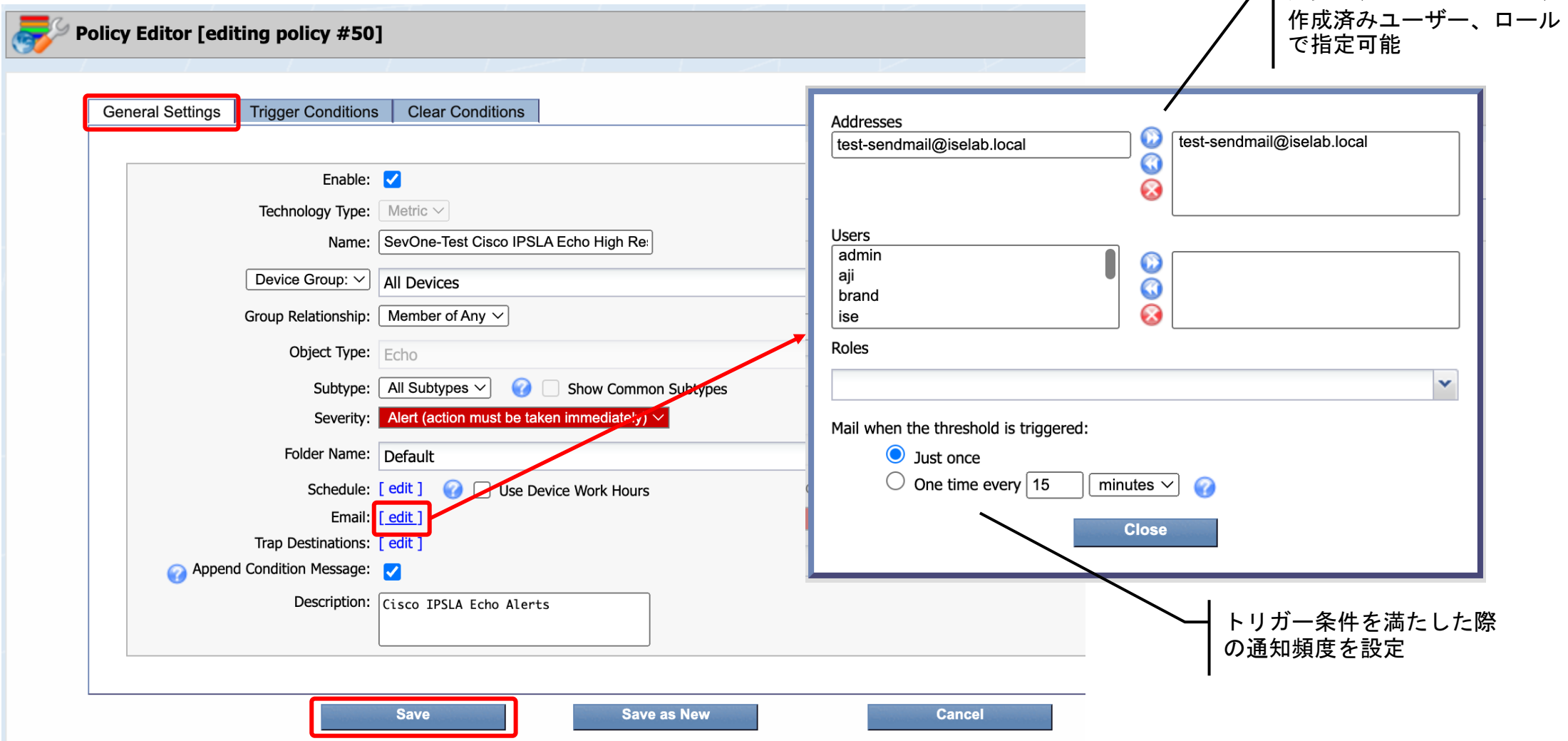


- [Cluster Settings] タブの左メニューより [Email] を選択し、メール・サーバーを設定



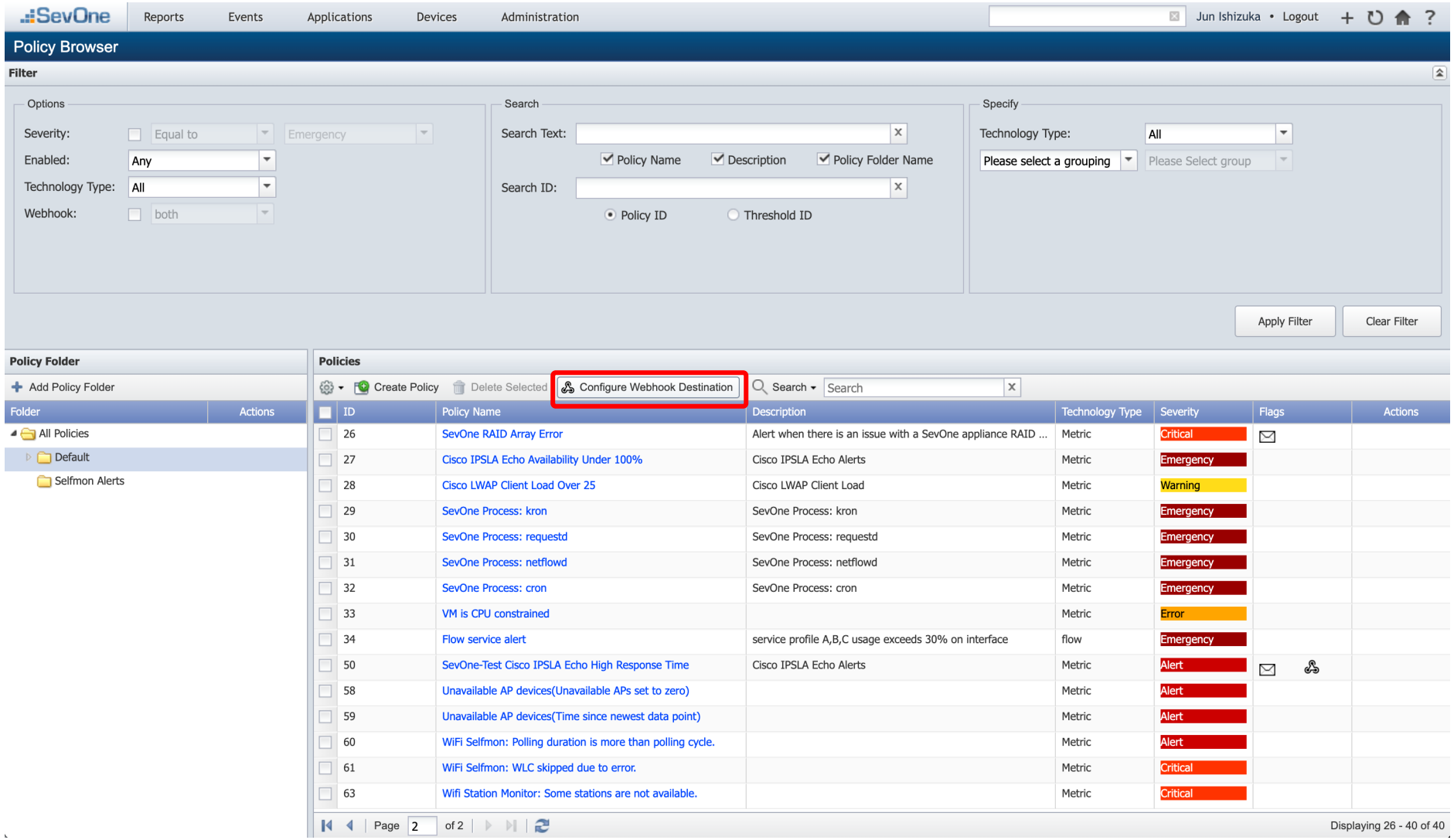
4.1.1.2. Email通知設定 (2/2)

- Policy Browserにて作成したPolicyの [General Settings] タブを開く
  - [Email] 欄の [edit] をクリックしてメール宛先を指定



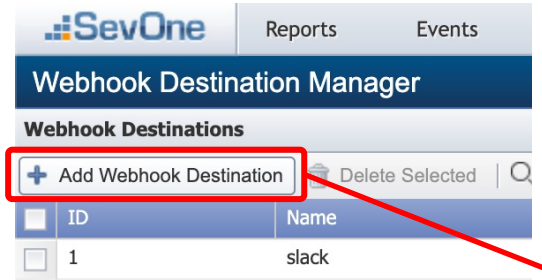
4.1.1.3. Webhook通知設定 (1/3)

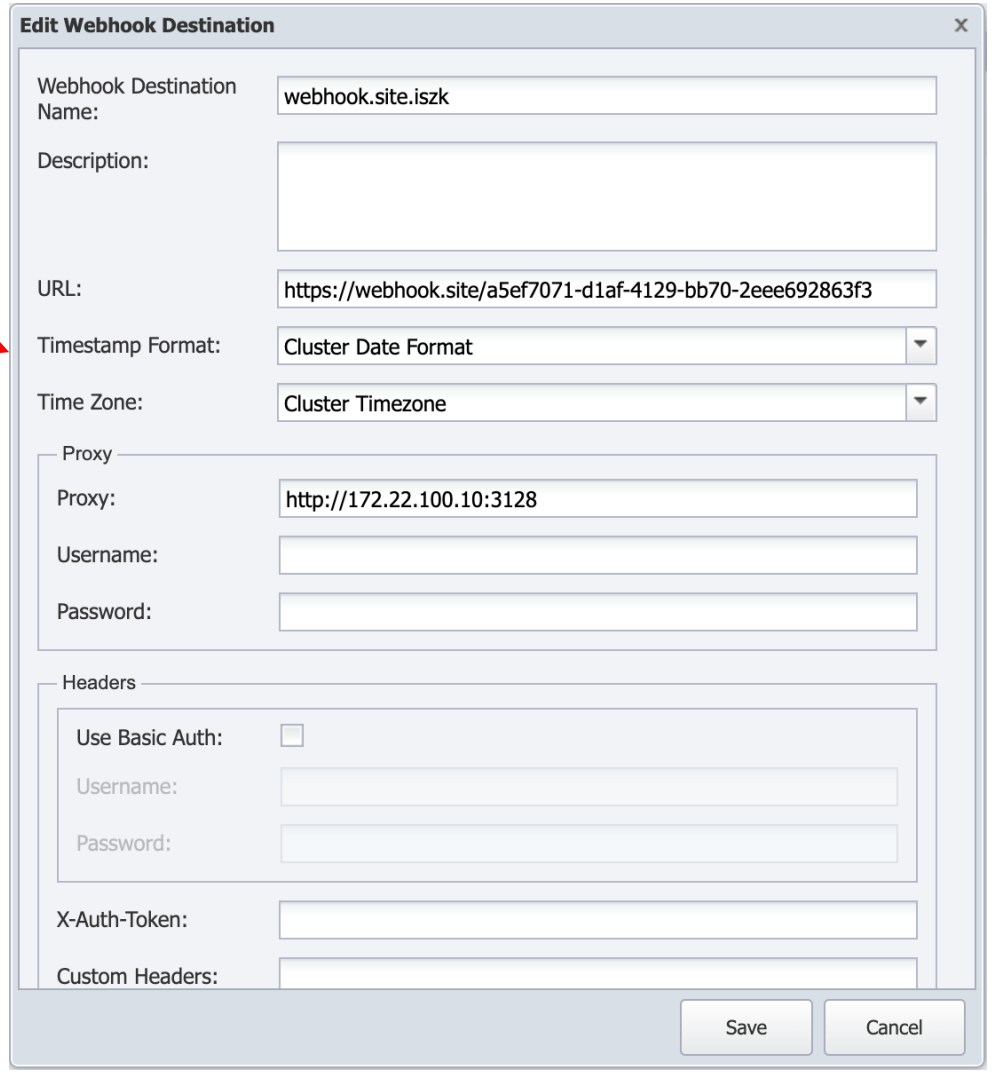
- Webhookの宛先設定
  - Policy Browserを開き、[Configure Webhook Destination] を選択



4.1.1.3. Webhook通知設定 (2/3)

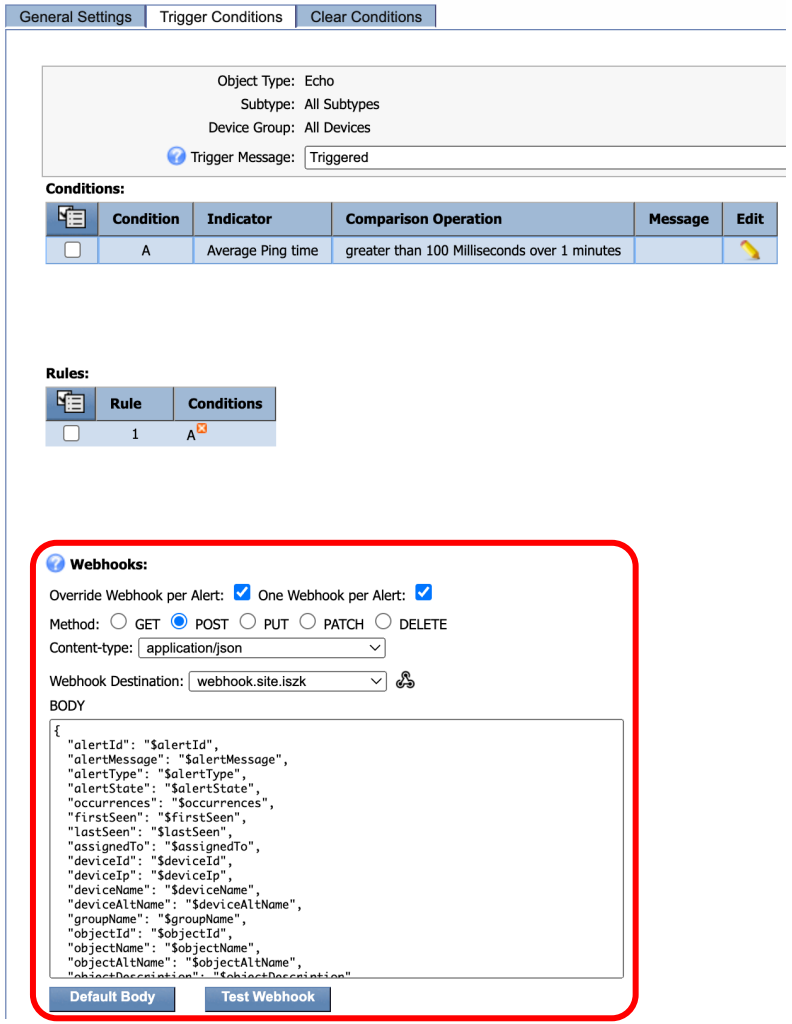
- Webhookの宛先設定
  - [Add Webhook Destination] を選択し、宛先URLなどを指定

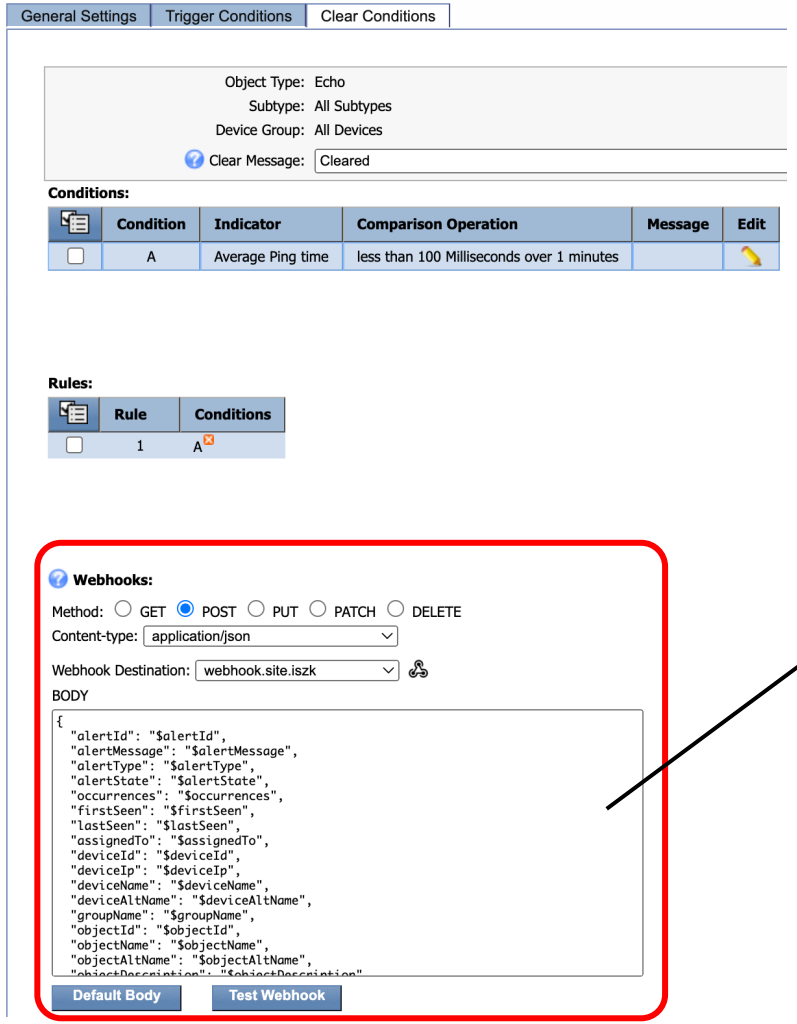




4.1.1.3. Webhook通知設定 (3/3)

- Webhookの宛先設定
  - 再度Policy Browserにて作成したPolicy開く
  - Webhookはトリガー時とクリア時のそれぞれで設定する

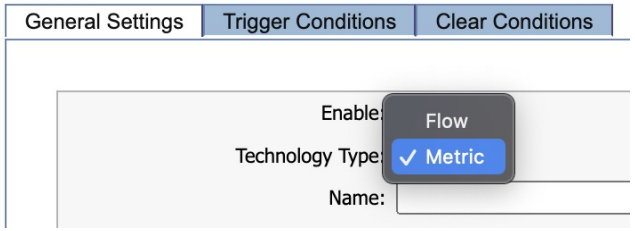




メッセージ・ボディーは
自由にカスタマイズ可能

(参考) WebhookのBODYで使用可能な変数

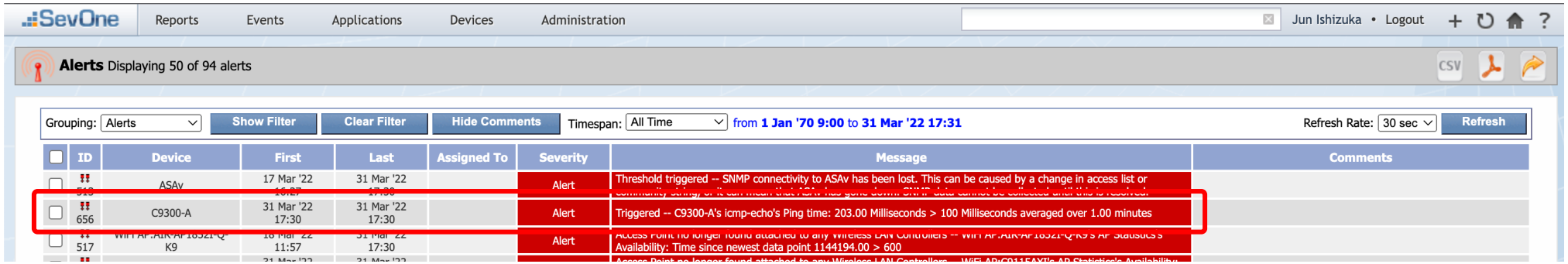
- Webhookではメッセージ・ボディーで以下の変数を指定可能
  - [Technology Type] によって使用できる変数が異なる
    - (*) は「Metric」のときのみ使用可



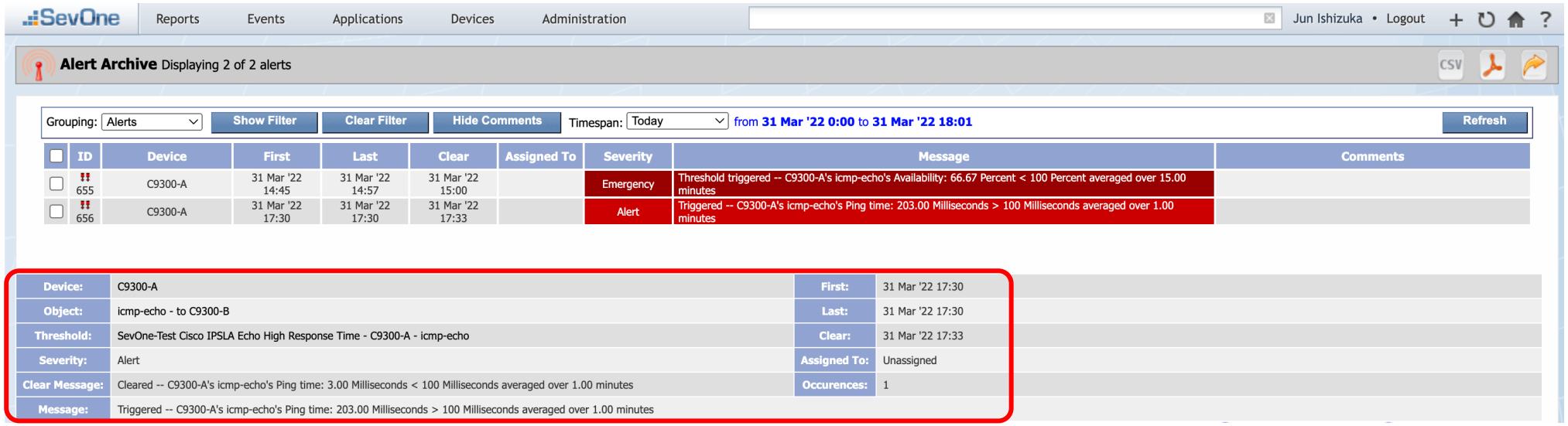
$alertId	アラートID
$alertMessage	アラート・メッセージ
$alertType	アラート・タイプ
$alertState	Severity (Emergency/Alert/Critical/Error/Warning/Notice/Info/Debug)
$occurrences	アラートがトリガーされた回数
$firstSeen	トリガーされた最初の日時
$lastSeen	トリガーされた最後の日時
$assignedTo	アラートがアサインされているユーザー
$deviceId	デバイスID
$deviceIp	デバイスのIPアドレス
$deviceName	デバイス名
$deviceAltName	デバイスの代替名
$groupName	デバイスグループ
$objectId (*)	オブジェクトID
$objectName (*)	オブジェクト名
$objectAltName (*)	オブジェクトの代替名
$objectDescription (*)	オブジェクトの説明
$pluginName (*)	プラグイン名（例: SNMP, IPSLA など）
$pluginDescription (*)	プラグインの説明
$policyId	ポリシーID
$policyName	ポリシー名
$thresholdId	しきい値ID
$thresholdName	しきい値名
$numTriggeringConditions (*)	トリガー条件の数
$triggeringConditions (*)	トリガー条件
$numConditions (*)	条件の数
$allConditions (*)	選択したContent-Typeに応じてフォーマットされたすべての条件の情報と計算値

4.1.2. アラート内容の確認

- トリガー条件を満たした際のアラート
  - [Events] > [Alerts]



- クリア条件を満たすと、上記 [Alerts] のリストから削除されアーカイブされる
  - [Events] > [Archives] > [Alert Archive]



4.1.2.1. Email通知内容 (1/2)

- トリガー条件を満たした際のEmail

```
Date: Thu, 31 Mar 22 08:30:16 +0000
Return-Path: sevone-admin@iselab.local
To: test-sendmail@iselab.local
From: SevOne Mailer <sevone-admin@iselab.local>
Subject: SevOne Alerts
Message-ID: <30af0edea5621d495209cb6a7ac314fb@localhost.localdomain>
X-Priority: 3
X-Mailer: PHPMailer 5.2.2 (http://code.google.com/a/apache-extras.org/p/phpmailer/)
MIME-Version: 1.0
Content-Transfer-Encoding: 8bit
Content-Type: text/plain; charset=UTF-8

Alert 656 - SEVERITY: Alert
                Triggered: 31 Mar '22 17:30
                Message: Triggered -- C9300-A's icmp-echo's Ping time: 203.00 Milliseconds > 100 Milliseconds averaged over 1.00 minutes


(this message was sent from SevOne Appliance.)
```

4.1.2.1. Email通知内容 (2/2)

■ クリア条件を満たした際のEmail

Date: Thu, 31 Mar 22 08:33:14 +0000
Return-Path: sevone-admin@iselab.local
To: test-sendmail@iselab.local
From: SevOne Mailer <sevone-admin@iselab.local>
Subject: CLOSED: SevOne Alerts
Message-ID: <7a21361274bee607596aecd662cfcd9e@localhost.localdomain>
X-Priority: 3
X-Mailer: PHPMailer 5.2.2 (http://code.google.com/a/apache-extras.org/p/phpmailer/)
MIME-Version: 1.0
Content-Transfer-Encoding: 8bit
Content-Type: text/plain; charset=UTF-8

Closed Alert 656 - SEVERITY: Alert
Closed: 31 Mar '22 17:30
Message: Cleared -- C9300-A's icmp-echo's Ping time: 3.00 Milliseconds < 100 Milliseconds averaged over 1.00 minutes
First Triggered: 31 Mar '22 17:30
Message: Triggered -- C9300-A's icmp-echo's Ping time: 203.00 Milliseconds > 100 Milliseconds averaged over 1.00 minutes

(this message was sent from SevOne Appliance.)

4.1.2.2. Webhook通知内容 (1/2)

■ トリガー条件を満たした際のWebhookのメッセージ・ボディー


```
{
 "alertId": "656",
 "alertMessage": "Triggered -- C9300-A's icmp-echo's Ping time: 203.00 Milliseconds > 100 Milliseconds averaged over 1.00 minutes",
 "alertType": "system",
 "alertState": "Alert",
 "occurrences": "1",
 "firstSeen": "31 Mar '22 17:30 Asia/Tokyo",
 "lastSeen": "31 Mar '22 17:30 Asia/Tokyo",
 "assignedTo": "unassigned",
 "deviceId": "153",
 "deviceIp": "172.22.11.93",
 "deviceName": "C9300-A",
 "deviceAltName": "",
 "groupName": "All Devices",
 "objectId": "6326",
 "objectName": "icmp-echo",
 "objectAltName": "",
 "objectDescription": "to C9300-B",
 "pluginName": "IPSLA",
 "pluginDescription": "IP SLA Poller",
 "policyId": "50",
 "policyName": "SevOne-Test Cisco IPSLA Echo High Response Time",
 "thresholdId": "2859",
 "thresholdName": "SevOne-Test Cisco IPSLA Echo High Response Time - C9300-A - icmp-echo",
 "numTriggeringConditions": "1",
 "triggeringConditions":
[{"aggregationDuration":"1.00","aggregationOperation":"Average","baselineValue":"0.00","comparisonOperation":">","comparisonUnits":">","comparisonValue":"100","dataUnits":"Milliseconds","
dataValue":"203.00","indicatorDescription":"Ping time","indicatorName":"echo_avgtime","sigmaDirection":"above","sigmaValue":"nan","thresholdValue":"100.00"}],
 "numConditions": "1",
 "allConditions":
[{"aggregationDuration":"1.00","aggregationOperation":"Average","baselineValue":"0.00","comparisonOperation":">","comparisonUnits":">","comparisonValue":"100","dataUnits":"Milliseconds","
dataValue":"203.00","indicatorDescription":"Ping time","indicatorName":"echo_avgtime","sigmaDirection":"above","sigmaValue":"nan","thresholdValue":"100.00"}]
}
```

4.1.2.2. Webhook通知内容 (2/2)

■ クリア条件を満たした際のWebhookのメッセージ・ボディー

```
{
 "alertId": "656",
 "alertMessage": "Triggered -- C9300-A's icmp-echo's Ping time: 203.00 Milliseconds > 100 Milliseconds averaged over 1.00 minutes",
 "alertType": "system",
 "alertState": "Alert",
 "occurrences": "1",
 "firstSeen": "31 Mar '22 17:30 Asia/Tokyo",
 "lastSeen": "31 Mar '22 17:30 Asia/Tokyo",
 "assignedTo": "unassigned",
 "deviceId": "153",
 "deviceIp": "172.22.11.93",
 "deviceName": "C9300-A",
 "deviceAltName": "",
 "groupName": "All Devices",
 "objectId": "6326",
 "objectName": "icmp-echo",
 "objectAltName": "",
 "objectDescription": "to C9300-B",
 "pluginName": "IPSLA",
 "pluginDescription": "IP SLA Poller",
 "policyId": "50",
 "policyName": "SevOne-Test Cisco IPSLA Echo High Response Time",
 "thresholdId": "2859",
 "thresholdName": "SevOne-Test Cisco IPSLA Echo High Response Time - C9300-A - icmp-echo",
 "numTriggeringConditions": "$numTriggeringConditions",
 "triggeringConditions": $triggeringConditions,
 "numConditions": "$numConditions",
 "allConditions": $allConditions
}
```