

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

1. 検証概要
2. SevOneインストール & セットアップ
 1. NMSのインストール & セットアップ
 2. SDIのインストール & セットアップ
3. ネットワーク監視
 1. SNMP
 2. IP SLA
 3. NBAR (Network-Based Application Recognition)
 4. xFlow
 5. Wi-Fi
- 4. イベント監視**
 - 1. Policy Browser**
5. Maps
 1. トポロジー
 2. ロケーション

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



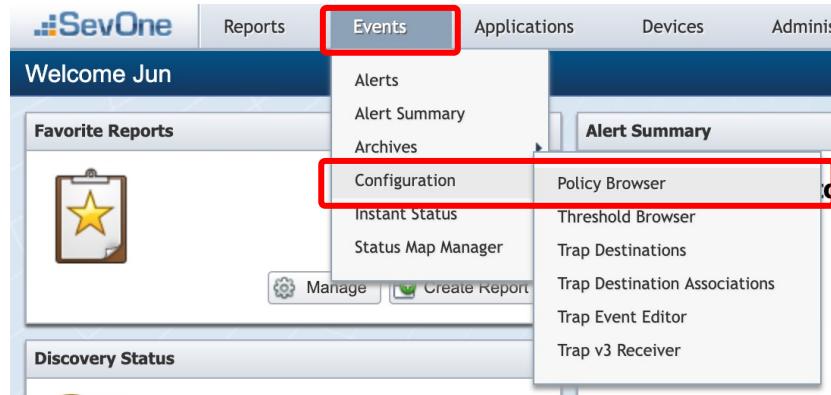
At present, Webhooks can only be configured on **Policies**. When adding **Thresholds**, although Webhooks are visible, they are **disabled** and cannot be configured.

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

SevOne Reports Events Applications Devices Administration Jun Ishizuka • Logout + ↺ 🏠 ?

Policy Browser

Filter

Options

Severity: ☐ Equal to Emergency

Enabled: Any

Technology Type: All

Webhook: ☐ both

Search

Search Text:

☒ Policy Name ☒ Description ☒ Policy Folder Name

Search ID:

☒ Policy ID ☐ Threshold ID

Specify

Technology Type: All

Please select a grouping Please Select group

Apply Filter Clear Filter

Policy Folder

+ Add Policy Folder

Folder Actions

- All Policies
- Default
- Selfmon Alerts

Policies

Create Policy Delete Selected Configure Webhook Destination Search Search

ID	Policy Name	Description	Technology Type	Severity	Flags	Actions
1	Ethernet Interface Traffic Over 95% - 32 Bit Counters	Ethernet Interface Traffic - 32 Bit Counters	Metric	Error		
2	Cisco IOS Memory Over 95%	Used Memory Alerts	Metric	Error		
3	Disk Over 90%	Generic Disk Used Alerts	Metric	Warning		
4	TCP Port Availability Under 100%	TCP Connect Alerts	Metric	Critical		
5	Website Alerts	Website Alerts	Metric	Alert		
6	ICMP Packet Loss Over 60%	ICMP Alerts	Metric	Emergency		
7	Cisco IPSLA Echo High Response Time	Cisco IPSLA Echo Alerts	Metric	Emergency		
8	Ethernet Interface Traffic Over 95% - 64 Bit Counters	Ethernet Interface Traffic - 64 Bit Counters	Metric	Error		
9	Interface Errors and Discards Over 100 in 15 Minutes	Interface Errors	Metric	Error		
10	CallManager Server Status	CallManager Server Status	Metric	Emergency		
11	Voice Gateway Status	Voice Gateway Status	Metric	Emergency		
12	CallManager Phone Status	CallManager Phone Status	Metric	Warning		
13	Cisco Temperature Over 50C	Temperature of devices running Cisco IOS	Metric	Alert		
14	Cisco CPU Over 85%	Devices running Cisco IOS	Metric	Warning		
15	Cisco Wireless AP Client Load Over 25	Cisco IOS Wireless	Metric	Warning		

Page 1 of 2

Displaying 1 - 25 of 40

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

The screenshot displays the IBM Automation Policy configuration interface. At the top, there are tabs for "General Settings", "Trigger Conditions" (highlighted with a red box), and "Clear Conditions". Below the tabs, the "Object Type" is set to "Echo", "Subtype" to "All Subtypes", and "Device Group" to "All Devices". The "Trigger Message" field is set to "Triggered" (highlighted with a red box). A note points to this field: "アラート・メッセージを指定可能".

Below the "Trigger Message" field, there is a "Conditions:" section with a table:

	Condition	Indicator	Comparison Operation	Message	Edit
☐	A	Average Ping time	greater than 100 Milliseconds over 1 minutes		

A red arrow points from the "Edit" icon to a detailed view of the condition configuration. This view shows the following settings:

- Indicator: Ping time
- Type: Static
- Comparison: greater than
- Threshold: 100 Milliseconds
- Duration: 1 minutes
- Aggregation: Average
- Custom Message: (empty field)

At the bottom of this view are "Save" and "Cancel" buttons. A note points to the "Save" button: "ここでは、1分間の平均RTTが100msを超えることをトリガー条件とする".

Below the "Conditions:" table, there is a "Rules:" section with a table:

	Rule	Conditions
☐	1	A 

A note points to the "Conditions" column: "複数の Condition を OR 条件で指定可能".

4.1.1.1. Policyの作成 (4/5)

- [Clear Conditions] タブを開き、同様に編集する

General Settings | Trigger Conditions | **Clear Conditions**

Object Type: Echo
Subtype: All Subtypes
Device Group: All Devices

Clear Message: Cleared 1017 characters remain

Conditions:

	Condition	Indicator	Comparison Operation	Message	Edit
☐	A	Average Ping time	less than 100 Milliseconds over 1 minutes		

Rules:

	Rule	Conditions
☐	1	A 

Indicator: Ping time

Type: Static

Comparison: less than

Threshold: 100 Milliseconds

Duration: 1 minutes

Aggregation: Average

Custom Message:

1024 characters remain

Save Cancel

ここでは、1分間の平均RTT
が100msを下回ることをク
リア条件とする

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

General Settings | Trigger Conditions | Clear Conditions

Enable: ☒

Technology Type: Metric

Name: SevOne-Test Cisco IPSLA Echo High Re

Device Group: All Devices

Group Relationship: Member of Any

Object Type: Echo

Subtype: All Subtypes ☐ Show Common Subtypes

Severity: Alert (action must be taken immediately)

Folder Name: Default

Schedule: [edit] ☐ Use Device Work Hours

Email: [edit]

Trap Destinations: [edit]

Append Condition Message: ☒

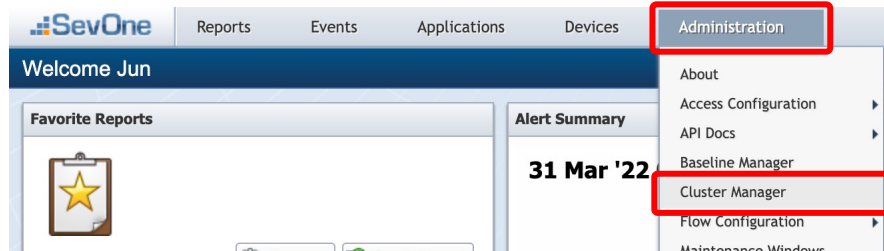
Description: Cisco IPSLA Echo Alerts

Save | Save as New | Cancel | Delete | Policy Browser

任意のSeverityを指定可能

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

A screenshot of the 'Cluster Settings' page in the SevOne interface. The 'Cluster Settings' tab is selected and highlighted with a red box. The left sidebar shows the 'Email' option highlighted with a red box. The main content area displays various email configuration settings:

- Email Server:** 172.22.11.170
- Username:** admin
- Password:** (masked with dots)
- Email Sender:** sevone-admin@iselab.local
- Email Sender Name:** SevOne Mailer
- Alerts Email Subject:** SevOne Alerts
- Reports Email Subject:** SevOne Report - \$name
- Multiple Alerts Per Email:** ☒
- Email Cleared Alerts:** ☒
- Connection Security:** None
- Port:** 25
- Compress Emailed Reports:** ☐
- Compress Reports Larger Than:** 5 MB
- Image Quality:** 10

At the bottom, there is a 'Send Test Email' button and 'Save' and 'Reset' buttons.

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

Policy Editor [editing policy #50]

General Settings | Trigger Conditions | Clear Conditions

Enable: ☒

Technology Type: Metric

Name: SevOne-Test Cisco IPSLA Echo High Re:

Device Group: All Devices

Group Relationship: Member of Any

Object Type: Echo

Subtype: All Subtypes ☐ Show Common Subtypes

Severity: Alert (action must be taken immediately)

Folder Name: Default

Schedule: [edit] ☐ Use Device Work Hours

Email: [edit]

Trap Destinations: [edit]

☒ Append Condition Message

Description: Cisco IPSLA Echo Alerts

Addresses

test-sendmail@iselab.local

test-sendmail@iselab.local

Users

admin
aji
brand
ise

Roles

Mail when the threshold is triggered:

☒ Just once

☐ One time every 15 minutes

Close

Save | Save as New | Cancel

宛先は、メールアドレス、作成済みユーザー、ロールで指定可能

トリガー条件を満たした際の通知頻度を設定

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

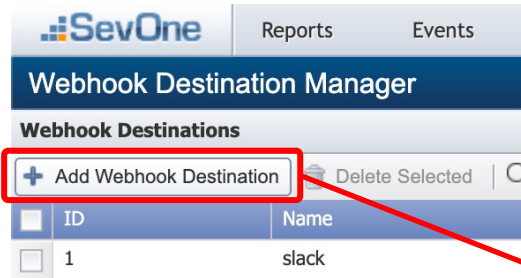
The screenshot shows the IBM Automation Policy Browser interface. The top navigation bar includes 'SevOne', 'Reports', 'Events', 'Applications', 'Devices', and 'Administration'. The user is logged in as 'Jun Ishizuka'. The 'Policy Browser' section is active, displaying a 'Filter' panel with options for Severity, Enabled, Technology Type, and Webhook. The 'Policies' table is shown below, with the 'Configure Webhook Destination' button highlighted in the table's header. The table lists various policies with columns for ID, Policy Name, Description, Technology Type, Severity, Flags, and Actions.

ID	Policy Name	Description	Technology Type	Severity	Flags	Actions
26	SevOne RAID Array Error	Alert when there is an issue with a SevOne appliance RAID ...	Metric	Critical	✉	
27	Cisco IPSLA Echo Availability Under 100%	Cisco IPSLA Echo Alerts	Metric	Emergency		
28	Cisco LWAP Client Load Over 25	Cisco LWAP Client Load	Metric	Warning		
29	SevOne Process: kron	SevOne Process: kron	Metric	Emergency		
30	SevOne Process: requestd	SevOne Process: requestd	Metric	Emergency		
31	SevOne Process: netflowd	SevOne Process: netflowd	Metric	Emergency		
32	SevOne Process: cron	SevOne Process: cron	Metric	Emergency		
33	VM is CPU constrained		Metric	Error		
34	Flow service alert	service profile A,B,C usage exceeds 30% on interface	flow	Emergency		
50	SevOne-Test Cisco IPSLA Echo High Response Time	Cisco IPSLA Echo Alerts	Metric	Alert	✉ 🔗	
58	Unavailable AP devices(Unavailable APs set to zero)		Metric	Alert		
59	Unavailable AP devices(Time since newest data point)		Metric	Alert		
60	WiFi Selfmon: Polling duration is more than polling cycle.		Metric	Alert		
61	WiFi Selfmon: WLC skipped due to error.		Metric	Critical		
63	Wifi Station Monitor: Some stations are not available.		Metric	Critical		

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



The 'Edit Webhook Destination' dialog box is shown. It has the following fields and options:

- Webhook Destination Name: webhook.site.iszk
- Description: (empty text area)
- URL: https://webhook.site/a5ef7071-d1af-4129-bb70-2eee692863f3
- Timestamp Format: Cluster Date Format (dropdown menu)
- Time Zone: Cluster Timezone (dropdown menu)
- Proxy section:
 - Proxy: http://172.22.100.10:3128
 - Username: (empty text field)
 - Password: (empty text field)
- Headers section:
 - Use Basic Auth: ☐
 - Username: (empty text field)
 - Password: (empty text field)
 - X-Auth-Token: (empty text field)
 - Custom Headers: (empty text field)

At the bottom right, there are 'Save' and 'Cancel' buttons.

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

General Settings | Trigger Conditions | Clear Conditions

Object Type: Echo
Subtype: All Subtypes
Device Group: All Devices
Trigger Message: Triggered

Conditions:

Condition	Indicator	Comparison Operation	Message	Edit
☐	A	Average Ping time	greater than 100 Milliseconds over 1 minutes	

Rules:

Rule	Conditions
☐ 1	A

Webhooks:

Override Webhook per Alert: ☒ One Webhook per Alert: ☒

Method: ☐ GET ☒ POST ☐ PUT ☐ PATCH ☐ DELETE

Content-type:

Webhook Destination:

BODY

```
{
  "alertId": "$alertId",
  "alertMessage": "$alertMessage",
  "alertType": "$alertType",
  "alertState": "$alertState",
  "occurrences": "$occurrences",
  "firstSeen": "$firstSeen",
  "lastSeen": "$lastSeen",
  "assignedTo": "$assignedTo",
  "deviceId": "$deviceId",
  "deviceIp": "$deviceIp",
  "deviceName": "$deviceName",
  "deviceAltName": "$deviceAltName",
  "groupName": "$groupName",
  "objectId": "$objectId",
  "objectName": "$objectName",
  "objectAltName": "$objectAltName",
  "objectDescription": "$objectDescription"
}
```

Default Body | Test Webhook

General Settings | Trigger Conditions | Clear Conditions

Object Type: Echo
Subtype: All Subtypes
Device Group: All Devices
Clear Message: Cleared

Conditions:

Condition	Indicator	Comparison Operation	Message	Edit
☐	A	Average Ping time	less than 100 Milliseconds over 1 minutes	

Rules:

Rule	Conditions
☐ 1	A

Webhooks:

Method: ☐ GET ☒ POST ☐ PUT ☐ PATCH ☐ DELETE

Content-type:

Webhook Destination:

BODY

```
{
  "alertId": "$alertId",
  "alertMessage": "$alertMessage",
  "alertType": "$alertType",
  "alertState": "$alertState",
  "occurrences": "$occurrences",
  "firstSeen": "$firstSeen",
  "lastSeen": "$lastSeen",
  "assignedTo": "$assignedTo",
  "deviceId": "$deviceId",
  "deviceIp": "$deviceIp",
  "deviceName": "$deviceName",
  "deviceAltName": "$deviceAltName",
  "groupName": "$groupName",
  "objectId": "$objectId",
  "objectName": "$objectName",
  "objectAltName": "$objectAltName",
  "objectDescription": "$objectDescription"
}
```

Default Body | Test Webhook

メッセージ・ボディは
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

The screenshot shows the 'Trigger Conditions' tab of a configuration window. Under 'Technology Type', a dropdown menu is open, displaying 'Flow' and 'Metric'. 'Metric' is selected, indicated by a blue checkmark. The 'Name' field below is empty.

\$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]

SevOne Alerts Displaying 50 of 94 alerts

Grouping: Alerts Show Filter Clear Filter Hide Comments Timespan: All Time from 1 Jan '70 9:00 to 31 Mar '22 17:31 Refresh Rate: 30 sec Refresh

ID	Device	First	Last	Assigned To	Severity	Message	Comments
558	ASAv	17 Mar '22 13:27	31 Mar '22 17:30		Alert	Threshold triggered -- SNMP connectivity to ASAv has been lost. This can be caused by a change in access list or community string, or it can mean that the device has gone down. This alert is generated when the device is unreachable.	
656	C9300-A	31 Mar '22 17:30	31 Mar '22 17:30		Alert	Triggered -- C9300-A's icmp-echo's Ping time: 203.00 Milliseconds > 100 Milliseconds averaged over 1.00 minutes	
517	WIFI AP: AIR-CT5502-K9	18 Mar '22 11:57	31 Mar '22 17:30		Alert	Access point no longer found attached to any Wireless LAN Controllers -- WIFI AP: AIR-CT5502-K9's AP Statistics's Availability: Time since newest data point 1144194.00 > 600	

- 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]

SevOne Alert Archive Displaying 2 of 2 alerts

Grouping: Alerts Show Filter Clear Filter Hide Comments Timespan: Today from 31 Mar '22 0:00 to 31 Mar '22 18:01 Refresh

ID	Device	First	Last	Clear	Assigned To	Severity	Message	Comments
655	C9300-A	31 Mar '22 14:45	31 Mar '22 14:57	31 Mar '22 15:00		Emergency	Threshold triggered -- C9300-A's icmp-echo's Availability: 66.67 Percent < 100 Percent averaged over 15.00 minutes	
656	C9300-A	31 Mar '22 17:30	31 Mar '22 17:30	31 Mar '22 17:33		Alert	Triggered -- C9300-A's icmp-echo's Ping time: 203.00 Milliseconds > 100 Milliseconds averaged over 1.00 minutes	

Device:	C9300-A	First:	31 Mar '22 17:30
Object:	icmp-echo - to C9300-B	Last:	31 Mar '22 17:30
Threshold:	SevOne-Test Cisco IPSLA Echo High Response Time - C9300-A - icmp-echo	Clear:	31 Mar '22 17:33
Severity:	Alert	Assigned To:	Unassigned
Clear Message:	Cleared -- C9300-A's icmp-echo's Ping time: 3.00 Milliseconds < 100 Milliseconds averaged over 1.00 minutes	Occurrences:	1
Message:	Triggered -- C9300-A's icmp-echo's Ping time: 203.00 Milliseconds > 100 Milliseconds averaged over 1.00 minutes		

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: <7a21361274bee607596aec662cfcd9e@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

```
{
  "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
}
```