

Zabbix 4.0

Non-Certified

Introductory Training

NTTCom Solutions 株式会社
マネジメントソリューション本部
プラットフォームソリューション部

福島 崇

パートナー有志で分担して新機能検証をする会
毎年恒例のお話になりますが、新バージョンがリリースされると
Zabbixパートナー企業のうちの有志が集って検証会を開催します。



IBM Japan
Systems
Engineering Co.,Ltd.

infocom



SRA OSS, INC.

NEC



Panasonic

パナソニック
ソリューションテクノロジー株式会社

FUJITSU

富士通ソーシャルサイエンスラボラトリ

Zabbix4.0の新機能については、我々にお尋ねください。

プレゼンの趣旨を簡単に説明すると.....

1. Zabbixの新バージョンリリース毎にワークショップやっています。
2. 今年はSRA OSSさんが新機能紹介を行ってくれるということに。
3. 切り口を変えてしまおう！
4. つまり今回のご紹介は「4.0 LTSの機能を活用して監視設定してみた」

ダッシュボードの改善

匠の手でリフォームされたダッシュボード

Dashboard ダッシュボードの変更

すべてのダッシュボード / Dashboard ズームアウト 最新の1時間

お気に入りのグラフ

- zbx30-dev-lldp.dc.zabicom.jp: CPU load
- zbx30-dev-lldp.dc.zabicom.jp: Disk space usage /
- zbx30-dev-lldp.dc.zabicom.jp: Network traffic on eth0

お気に入りのスクリーン

- Port List
- Zabbix server

お気に入りのマップ

- Local network
- ホストグループ集約マップ (サブグループ)

障害

時間	復旧時刻	ステータス	情報	ホスト	障害・深刻度	継続期間	確認済	アクション
2018/10/24 16:41:35		障害	ひみつ	W-ZL2SW03 - DGS-1100-24	[Port - {#PORT_NAME}] - Link Down	13d 23h 7m	いいえ	
2018/10/24 16:41:35		障害	ひみつ	W-ZL2SW03 - DGS-1100-24	[Port - {#PORT_NAME}] - Link Down	13d 23h 7m	いいえ	
2018/10/24 16:41:35		障害	ひみつ	W-ZL2SW03 - DGS-1100-24	[Port - {#PORT_NAME}] - Link Down	13d 23h 7m	いいえ	
2018/10/24 16:41:35		障害	ひみつ	W-ZL2SW03 - DGS-1100-24	[Port - {#PORT_NAME}] - Link Down	13d 23h 7m	いいえ	

障害中のホスト

ホストグループ	障害なし	障害あり	合計
Discovered hosts	38	22	60
lldp_test		5	5
Network Device (FreeVersion)		2	2
Network Device (LLDP not supported)	38	19	57
Network Device (LLDP supported)	6	15	21
Zabbix servers	1		1

深刻度ごとの障害数

ホストグループ	致命的な障害	重度の障害	軽度の障害	警告	情報	未分類
Discovered hosts			1			295
lldp_test						87
Network Device (FreeVersion)						38
Network Device (LLDP not supported)			1			230
Network Device (LLDP supported)						288
Zabbix servers						

システム情報

パラメータ 値 詳細

ウィジェットのサイズ/配置も自由自在

ドラッグ操作で
拡大/縮小も自由自在

お気に入りのスクリーン

- Port List
- Zabbix server

お気に入りのマップ

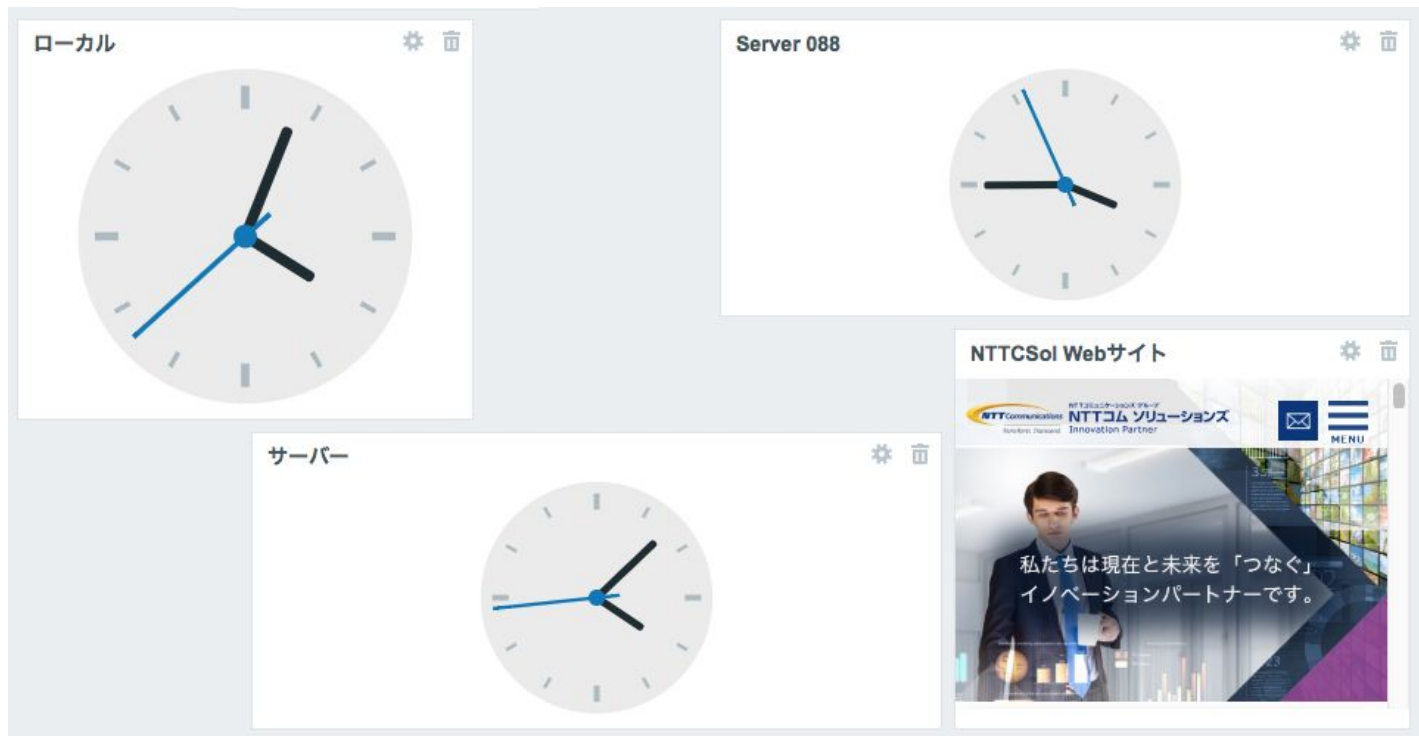
- Local network
- ホストグループ集約マップ (サンプル)

障害中の...

- ホストグル
- Discovered
- lldp_test
- Network De
- Network De
- Network De
- Zabbix serv

ホスト	障害・深刻度	継続期間	確認済	アクション
000113-WZ12SW03-DCS-1100	IPset: #PORT_NAME1 Link	13d 23h 10m	いい	

いままででは難しかった無駄の多い柔軟な配置が可能

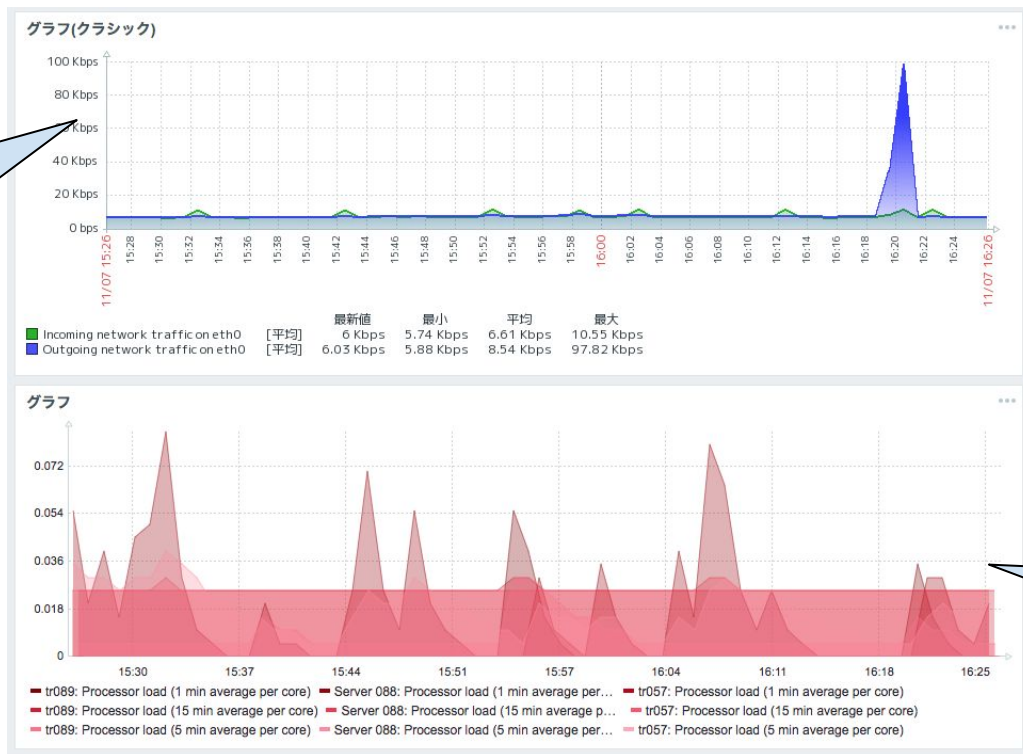


新しいグラフウィジェット



見た目ではさほどの変化はないが.....

昔からある
ウィジェット



新しい
ウィジェット

複数アイテムを簡単にグラフに描画可能

データセット 表示オプション 期間 軸 凡例 障害 オーバーライド

データセット 選択 CPU* 選択 ×

基本色

グラフの形式 線 ポイント 棒グラフ

欠損データ なし 接続する 0とみなす

Y軸 左 右

タイムシフト

透明度

塗りつぶし

1

3

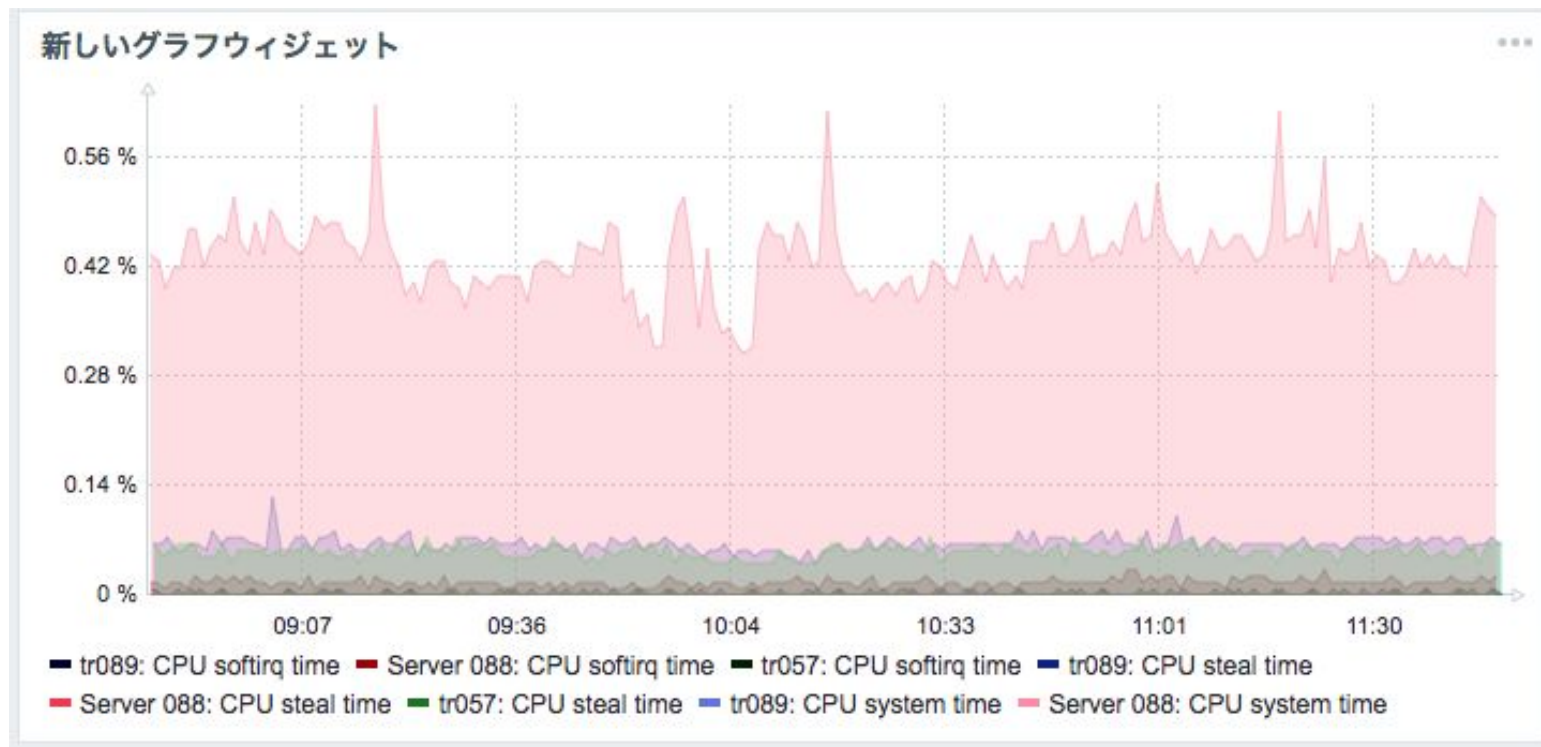
5

3

ワイルドカードとカンマ区切りを
駆使して複数指定

タイムシフトが利用可能に！

こんな素敵グラフがあったという間に完成



タイムシフトが使えるということは

予測トリガーを使った計算アイテム

* 名前

タイプ

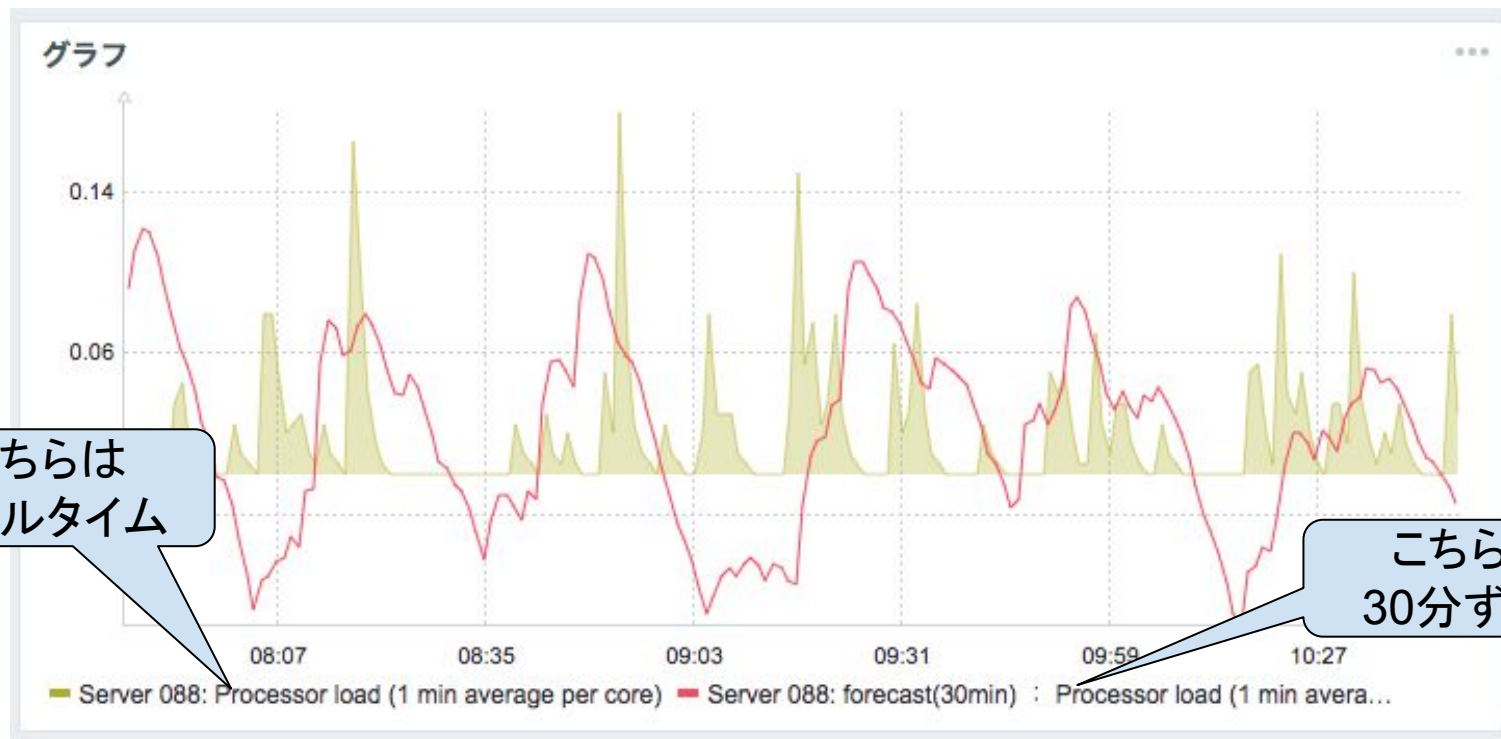
* キー

* 式

データ型

直近30分のヒストリを元に、30分後の未来の値を予測

30分タイムシフトして描画すると.....



■ そういえば、よく似た機能が既にあったような.....？



スクリーンさん

俺.....最近 影薄くね？

ダッシュボード 1強時代にはまだ至っていない

	スクリーン	ダッシュボード
ウィジェットの種類	たくさん	たくさん+新しいグラフ
配置	セル合わせ	完全に自由
「共有」によるアクセス制御	できる	できる
スライドショー	使える	使えない
設定をXMLでエクスポート	できる	できない

グラフの話が出たので余談ですが

マップ(とダッシュボードの新しいグラフウィジェット)の描画方法が
PNG形式で出力 ⇒ SVG(Scalable Vector Graphics)形式で出力に変更



「名前をつけて画像を保存」
が無い！！

イベント相関関係を用いた障害管理

イベントにはタグを付けられるようになりました

トリガーの設定画面に「タグ」という設定項目が追加されています。

正常時のイベントクローズ **すべての障害** タグの値が一致したすべての障害

タグ

TAG	Heuer	削除
Tug	boat	削除
タグ	ラグビー	削除
タグ	値	削除

追加

手動クローズを許可

タグの名称

タグの値

詳細は SRA OSSさんのプレゼンを思い出してね☆

「正常時のイベントクローズ」! ?

トリガーの設定画面に「タグ」という設定項目が追加されています。

正常時のイベントクローズ

すべての障害 タグの値が一致したすべての障害

タグ	タグの値	削除
Heuer		削除
		削除
タグ	ラグビー	削除
タグ	値	削除

追加

手動クローズを許可

タグの名称

タグの値

みなさんよく見かけるこんなログ

```
Zabbix agent item "vm.memory.size[available]" on host "tr057" failed: first network error, wait for 15 seconds  
temporarily disabling Zabbix agent checks on host "tr057": host unavailable  
Zabbix agent item "agent.ping" on host "tr089" failed: first network error, wait for 15 seconds  
temporarily disabling Zabbix agent checks on host "tr089": host unavailable  
enabling Zabbix agent checks on host "tr057": host became available  
enabling Zabbix agent checks on host "tr089": host became available
```

/var/log/zabbix/zabbix_server.log より

トリガー付けてイベントに残したいな

「復旧条件式」を活用

* 名前 **「障害」イベントを生成する条件**

深刻度 未分類 情報 警告 軽度の障害 重度の障害 致命的な障害

* 障害の条件式

条件式ビルダー

正常イベントの生成 条件式 復旧条件式 なし

* 復旧条件式

条件式ビルダー

障害イベント生成モード 単一 複数

正常時のイベントクローズ すべての障害 タグの値が一致したすべての障害

タグ

見事障害を検知

[監視データ]⇒[最新データ]⇒ ヒストリ

Zabbix4.0サーバ: ログ監視[/var/log/zabbix/zabbix_sever.log]

タイムスタンプ	ローカル時間	値
2018/11/09 09:57:03	18667:20181108:145640.671	temporarily disabling Zabbix agent checks on host "tr057": host unavailable
2018/11/09 09:53:38	18665:20181108:145540.939	Zabbix agent item "vm.memory.size[available]" on host "tr057" failed: first network error, wait for 15 seconds

[監視データ]⇒[障害]

時間 ▼	<input type="checkbox"/> 深刻度	復旧時刻	ステータス	情報	ホスト	障害
09:57:03	<input type="checkbox"/> 重度の障害		障害		Zabbix4.0サーバ	[tr057] の監視状況アラートを検知しました

{ITEM.VALUE}.regsub()
の活躍に注目

別のホストのnetwork errorが発生しても.....

[監視データ]⇒[最新データ]⇒ヒストリ

Zabbix4.0サーバ: ログ監視[/var/log/zabbix/zabbix_sever.log]

タイムスタンプ	ローカル時間	値
2018/11/09 10:03:59	18664:20181108:145643.031	Zabbix agent item "agent.ping" on host "tr089" failed: first network error, wait for 15 seconds
2018/11/09 09:57:03	18667:20181108:145640.671	temporarily disabling Zabbix agent checks on host "tr057": host unavailable
2018/11/09 09:53:38	18665:20181108:145540.939	Zabbix agent item "vm.memory.size[available]" on host "tr057" failed: first network error, wait for 15 seconds

[監視データ]⇒[障害]

時間 ▼	<input type="checkbox"/> 深刻度	復旧時刻	ステータス	情報	ホスト	障害
09:57:03	<input type="checkbox"/> 重度の障害		障害		Zabbix4.0サーバ	【tr057】の監視状況アラートを検知しました

「復旧条件式」に合致しないので復旧しない

別のホストもUnavailableになったら.....

[監視データ]⇒[最新データ]⇒ ヒストリ

Zabbix4.0サーバ: ログ監視[/var/log/zabbix/zabbix_sever.log]

タイムスタンプ	ローカル時間	値
2018/11/09 10:14:20	18667:20181108:145743.687	temporarily disabling Zabbix agent checks on host "tr089": host unavailable
2018/11/09 10:03:59	18664:20181108:145643.031	Zabbix agent item "agent.ping" on host "tr089" failed: first network error, wait for 15 seconds
2018/11/09 09:57:03	18667:20181108:145640.671	temporarily disabling Zabbix agent checks on host "tr057": host unavailable
2018/11/09 09:53:38	18665:20181108:145540.939	Zabbix agent item "vm.memory.size[available]" on host "tr057" failed: first network error, wait for 15 seconds

[監視データ]⇒[障害]

時間 ▼	<input type="checkbox"/> 深刻度	復旧時刻	ステータス	情報	ホスト	障害
10:14:20	<input type="checkbox"/> 重度の障害		障害		Zabbix4.0サーバ	[tr089] の監視状況アラートを検知しました
10:00						
09:57:03	<input type="checkbox"/> 重度の障害		障害		Zabbix4.0サーバ	[tr057] の監視状況アラートを検知しました

「障害イベント生成モード」が「複数」なのでちゃんと検知

もちろんtr089が復旧してもしっかり検知！

[監視データ]⇒[最新データ]⇒ ヒストリ

Zabbix4.0サーバ: ログ監視[/var/log/zabbix/zabbix_sever.log]

タイムスタンプ	ローカル時間	値
2018/11/09 10:19:13	18667:20181108:145943.723	enabling Zabbix agent checks on host "tr089": host became available
2018/11/09 10:14:20	18667:20181108:145743.687	temporarily disabling Zabbix agent checks on host "tr089": host unavailable
2018/11/09 10:03:59	18664:20181108:145643.031	Zabbix agent item "agent.windo" on host "tr089" failed: first network error. wait for 15 seconds

[監視データ]⇒[障害]

時間	<input type="checkbox"/> 深刻度	復旧時刻	ステータス	情報	ホスト	障害
10:14:20	<input type="checkbox"/> 重度の障害	10:19:13	解決済		Zabbix4.0サーバ	[tr089] の監視状況アラートを検知しました
10:00	<input checked="" type="checkbox"/> 重度の障害					
09:57:03	<input type="checkbox"/> 重度の障害	10:19:13	解決済		Zabbix4.0サーバ	[tr057] の監視状況アラートを検知しました

ぐわー！ tr089だけじゃなくtr057も復旧しちゃった！！

どうやらトリガー設定の「タグ」が重要らしい

```
{{ITEM.VALUE1}.regex("on host \"([A-Za-z0-9\._-]+)\", \1)}
```

障害イベント生成モード 半 複数

正常時のイベントクローズ すべての障害 タグの値が一致したすべての障害

タグ

ホスト名	<input ([a-za-z0-9\._-]+)\",="" \1)"="" type="text" value='{{ITEM.VALUE1}.regex("on host \'/>	削除
監視内容	<input type="text" value="通信可否"/>	削除

[追加](#)

手動クローズを許可

生成されるイベントに設定したとおりのタグが付く

時間	深刻度	復旧時刻	ステータス	情報	ホスト	障害	継続期間	確認済	アクション	タグ
11:04:14	<input type="checkbox"/>		重度の障害		Zabbix4.0サーバ	【tr089】の監視状況アラートを検知しました	5s	いいえ		ホスト名: tr089 監視内容: 通信可否

タグ

ホスト名: tr089 監視内容: 通信可否

マクロも名前解決済み

トリガーの設定でこのタグを利用します

障害イベント生成モード 単一 複数

正常時のイベントクローズ すべての障害 タグの値が一致したすべての障害

* クローズに利用するタグ名

タグ	監視内容	削除
<input type="text" value="ホスト名"/>	<input type="text" value="{{ITEM.VALUE1}.regsub('on host \\'([A-"/>	削除
<input type="text" value="監視内容"/>	<input type="text" value="通信可否"/>	削除

自分で「タグ」で定義した「タグ名」と同じものを指定

今度は見事に tr089 だけが「解決済み」に！

時間	深刻度	復旧時刻	ステータス	情報	ホスト	障害	継続期間	確認済	アクション	タグ
11:42:27	<input type="checkbox"/>		解決済		Zabbix4.0サーバ	【tr089】の監視状況アラートを検知しました	32s	いいえ		ホスト名: tr089 監視内容: 通信可否
11:41:25	<input type="checkbox"/>		障害		Zabbix4.0サーバ	【tr057】の監視状況アラートを検知しました	1m 37s	いいえ		ホスト名: tr057 監視内容: 通信可否

ステータス

- 解決済
- 障害

【tr089】の監視状況アラートを検知しました

【tr057】の監視状況アラートを検知しました

ホスト名: tr089 監視内容: 通信可否

ホスト名: tr057 監視内容: 通信可否

「ホスト名」タグの一致する
イベントだけがクローズされる

まとめると.....

1. トリガーの設定画面に「タグ」という設定項目が追加されています。
2. タグにはマクロが利用できます。
3. マクロ入りタグをうまく設定すると、同じトリガーから生成されたイベントであっても別個に障害/復旧の判定ができます。
4. いままでのZabbixでは弱かったログ監視が大幅に強化できる！？

異なるトリガーから生成されたイベントも使いたい！



「設定」⇒「イベント相関関係」から
グローバルな(トリガーをまたいだ)相関関係を
作ることが可能

「相関関係」タブで、タグ同士のつながりを定義

イベント相関関係ルール

相関関係 実行内容

* 名前

* 実行条件

ラベル	名前	アクション
新規条件	<input type="checkbox"/> 古いイベントのタグ <input type="checkbox"/> 新しいイベントのタグ <input type="checkbox"/> 新しいイベントのホストグループ <input type="checkbox"/> イベントタグのペア <input type="checkbox"/> 古いイベントのタグの値 <input type="checkbox"/> 新しいイベントのタグの値	等しい <input type="text" value="タグ"/>

説明

有効

「実行内容」タブで、新旧どちらをクローズするのか

イベント相関関係ルール

相関関係 実行内容

* 実行内容

詳細

アクション

古いイベントのクローズ

[削除](#)

実行内容の追加

新しいイベントのクローズ ▾

[追加](#)

追加

キャンセル

応用例としては？



あ！
これをうまく使えばトラップ監視でも
例えばインターフェースのUp/Downを
簡単に表現できるんじゃないか？

そんな面倒なことをするくらいならLLD使いましょうよ

■ディスカバリルール

* 名前	Network Interfaces Discovery
タイプ	SNMPv2エージェント
* キー	net.if.discovery
* SNMP OID	discovery{{#IFOPERSTATUS}},1.3.6.1.2.1.2.2.1.8,{{#IFADMINSTATUS}},1.3.6.1.2.1.2
* SNMPコミュニティ	{\${SNMP_COMMUNITY}}

※ 標準テンプレートの『Template Module Interfaces SNMPv2』に設定されている
ディスカバリルール『 Network Interfaces Discovery』と同じルール

アイテムのプロトタイプ

■SNMPトラップ受信アイテム

名前	<input type="text" value="【#IFNAME】 SNMPトラップ"/>
タイプ	<input type="text" value="SNMPトラップ"/>
キー	<input type="text" value="snmptrap[{#IFNAME}]"/>

トラップ監視にもLLDを活用しよう

トリガーのプロトタイプ

■インターフェースの Link Up/Down

* 名前

深刻度

* 障害の条件式

条件式ビルダー

正常イベントの生成

* 復旧条件式

条件式ビルダー

障害イベント生成モード

linkDownのTrapが飛んできたら障害

linkUpのTrapが飛んできたら正常

手動クローズを許可 Trapは飛んでこない事があるので.....



ご清聴ありがとうございました



IBM Japan
Systems
Engineering Co.,Ltd.



パナソニック
ソリューションテクノロジー株式会社



富士通ソーシャルサイエンスラボラトリ