50th Anniversary SINCE1970 and always will be

オンプレ監視のクラウド移行における Zabbixでの体験談

2020年11月14日

株式会社セゾン情報システムズ
カスタマーサービスセンター
伊原　翔馬

Agenda

1. 自己紹介
2. 会社紹介
3. SAIMONサービス紹介
4. Zabbix導入にあたって
5. クロージング

自己紹介

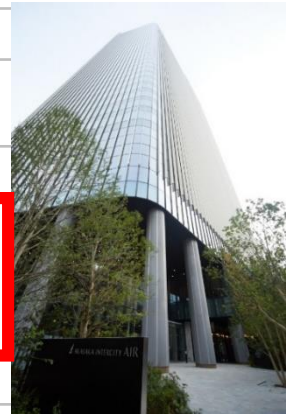
■ 伊原　翔馬

- 株式会社セゾン情報システムズ　2017年入社
- 24歳。まだまだ若手です
- 普段はシステム運用をしています。
  一部システムでは開発も担当しています
- Zabbix 4.0 Certified Professionalの試験突破しました
- 好きなZabbixの機能：タグ
  特定トリガーのメンテナンス、
  アクションのタグ指定による通知先の制御
  など用途多数！

会社紹介

● 会社概要

商　　号	株式会社セゾン情報システムズ
設立年月日	1970 年 9 月 1 日
表取締役　社長	内　田　和　弘
資　本　金	1,367百万円
事業内容	‣ フィナンシャルITサービスビジネス ‣ 流通ＩＴサービスビジネス ‣ リンケージビジネス ‣ HULFTビジネス
従業員数	749名（2020年 9月末現在　連結）
本社所在地	東京都港区赤坂一丁目8番1号
上場市場	東京証券取引所JASDAQスタンダード市場（9640）
主要株主（上位3位）	‣ 株式会社クレディセゾン ‣ イーシーエム エムエフ ‣ イーシーエム　マスターファンド　エスピーブイワン
認定・届出	総務省　電気通信事業者届出
品質 セキュリティ	‣ プライバシーマーク付与認定取得 ・登録番号 【11820059】 ‣ JISQ27001:2014（ISO/IEC27001:2013） 認証取得 ・登録番号 【JMAQA-S030】



1970年　㈱西武情報センター設立・創業
西武流通グループ（当時）の情報処理機能の統合と新しい情報サービス業の創造を目的として設立。情報処理サービス事業、ソフトウェア開発事業を開始。

1992年　㈱セゾン情報システムズに商号変更

1993年　JASDAQスタンダードに上場
通信ミドルウェア「HULFT」販売開始
業種・業界を問わず広汎に利用され、国内シェア第1位の実績を誇るファイル連携ミドルウェアの販売開始。

2005年　世存信息技術（上海）有限公司を設立
中国における生産拠点として位置づけ、上海に現地法人を設立。

2010年　クラウド関連製品・サービス提供開始
セキュアWebデータ連携ミドルウェア「HULFTクラウド（現HULFT-WebFileTransfer）」、クラウド型ホスティングサービス「SAISOS」を提供開始。クラウド＆グローバル時代に求められるニーズに対応するための技術・環境を整備。

2013年　㈱アプレッソ株式を取得、子会社化
データ連携ソリューションの強化とともに、先端技術の研究開発経営の基盤を醸成。

2015年　ASEAN拠点 HULFT Ｐｔｅ．Ｌｔｄ.設立
グローバルビジネス拡大を図るため、 ASEAN地域を設立。

2016年　北米拠点 HULFT, Inc.を設立
グローバルビジネス拡大を図るため、北米拠点を設立。
米国開催 AWS re:Invent 2015で「Think Big」賞を受賞。

2017年　EMEA事務所を設立
グローバルビジネス拡大を図るため、EMEAエリア（ヨーロッパ、中東、アフリカ地域）拠点を設立。

本社所在地を 東京都港区赤坂に移転

2018年　㈱フェスをIDホールディングスに譲渡

2019年　㈱アプレッソを吸収合併
パッケージソフトウェア開発・販売強化のため合併。

SAIMONサービスについて

情報システムの重要性が高まりつつある昨今、業務システムの安定稼働のために
企業では多くの人員やコストが割かれています。
クラウド対応型の統合運用監視サービス「SAIMON」は、システム管理に関わる手間
や負担を減らしお客様本来の業務に注力できるようサポートをするサービスです。
サーバやネットワークの正常性確認・異常通知を行う「監視サービス」とお客様の
監視業務を代行する「運用サービス」を**24時間365日体制でご提供します！**

監視サービス

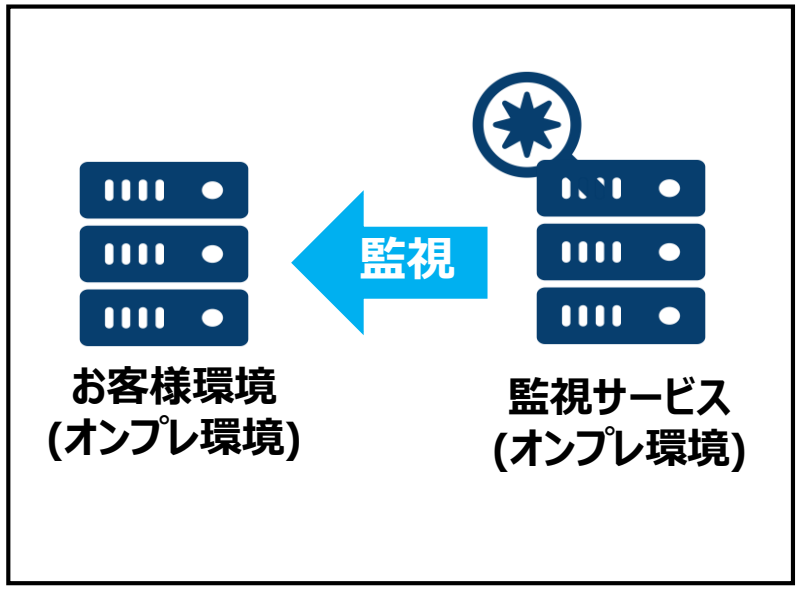
運用サービス

SAIMONサービス概要

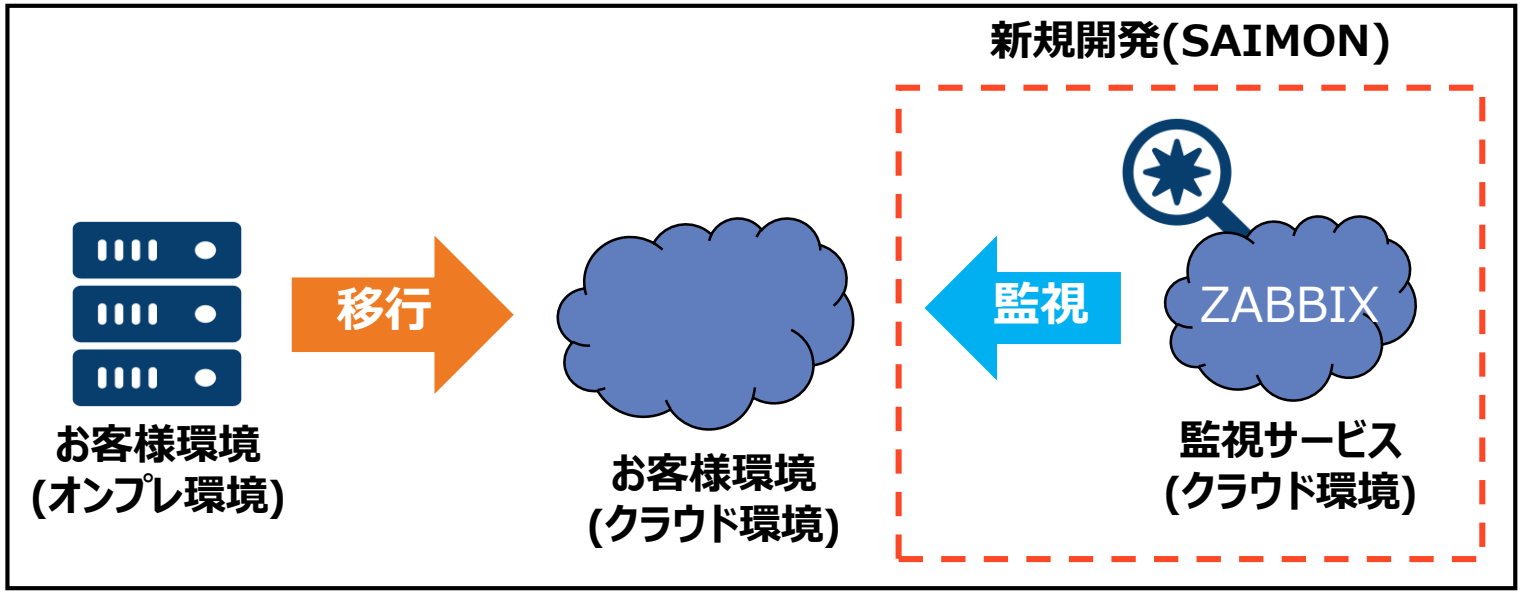
多種多様な監視対象コンポーネントに対し、死活監視やログ監視を実装し異常が発生した場合はメールやSlackによる通知と架電連絡を行います。必要なオペレーションについては代行しますが、監視システムのWebダッシュボードを用意しユーザ自身でも実行可能な環境をご提供します。

SAIMON開発の背景

従来



クラウド対応



- お客様環境(オンプレ環境)の監視を提供していたが、お客様環境のクラウド移行に伴い監視サービスもクラウド対応が必要
- クラウドネイティブなSaaS監視製品では対応できない要件があった
  (オンプレのサーバをクラウド上にシフトしただけの環境もあったため、監視要件はオンプレと同様)

⇒クラウド対応可能かつ監視要件を満たせるOSS(Zabbix)を利用し、クラウド対応の監視サービスを開発

なぜZabbixを選んだのか？

- クラウド環境で動作する

- ライセンス課金でない
  - 初期コストを抑えられる
  - 顧客の流動性に柔軟に対応できる

- 監視要件を満たすことができる
  - 移行前の監視要件と同様の監視を実現できる

- 監視システムのOSSの中で最も開発が活発
  - ユーザが多く、コミュニティも活発であるため、疑問点を自己解決できる

- Zabbix Japan様のサポートサービスがある
  - 日本語・日本時間でのサポートが受けられる

Zabbix導入にあたり苦労・工夫した点

- 監視要件
  - 監視内容はサーバ単位で個別に指定可能
    (監視内容：監視するリソースとそのしきい値、監視するログと監視文字列等)
  - 障害発生時にアラート通知可能
  - アラート通知はメール通知・電話通知が設定可能
  - 監視内容の重要度により通知先の振り分けが可能
  - 監視の一時停止・監視除外時間の設定が可能
  - お客様からの依頼に基づく監視内容の変更が可能
  - ログ監視において検知したエラーログは漏れなく通知する
  - ログ監視においてログのフィルタリングが可能(監視除外文字列の指定が可能)
  - 大量アラートが発生した場合、アラート通知を抑止する

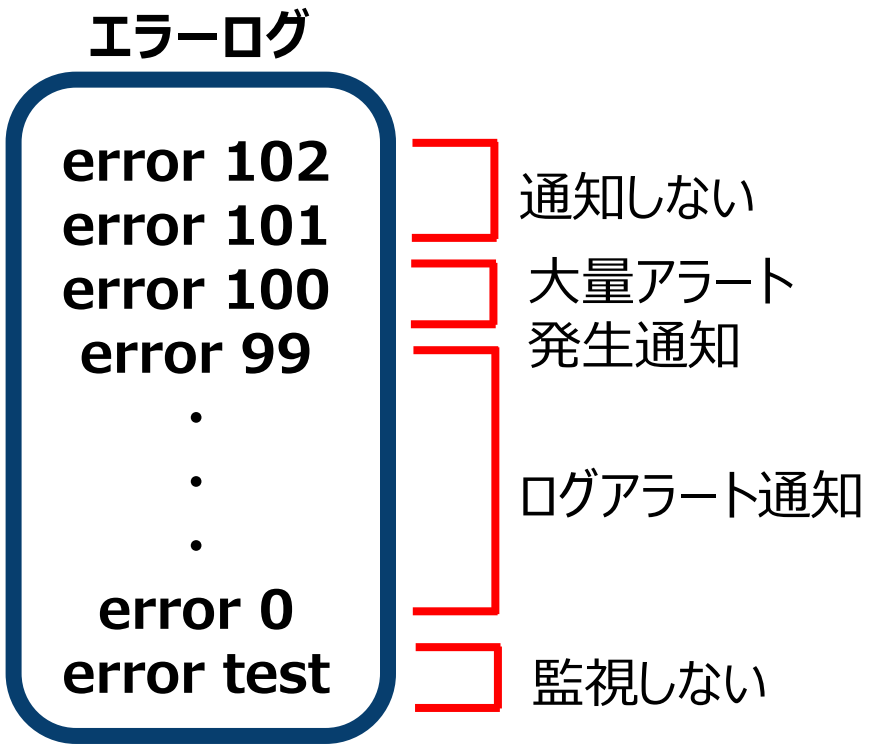
Zabbix導入にあたり苦労・工夫した点

- 監視要件
  - ログ監視において検知したエラーログは漏れなく通知する
  - ログ監視においてログのフィルタリングが可能(監視除外文字列の指定が可能)
  - 大量アラートが発生した場合、アラート通知を抑止する

- ログ監視の動作

監視内容

監視文字列：	error
	warn
監視除外文字列：	info
	test



⇒ログ監視設計
1. 障害イベントの複数設定
2. 監視除外文字列の指定
3. 監視文字列の指定
4. 大量ログアラートの抑止

ログ監視設計

1. 障害イベントの複数設定

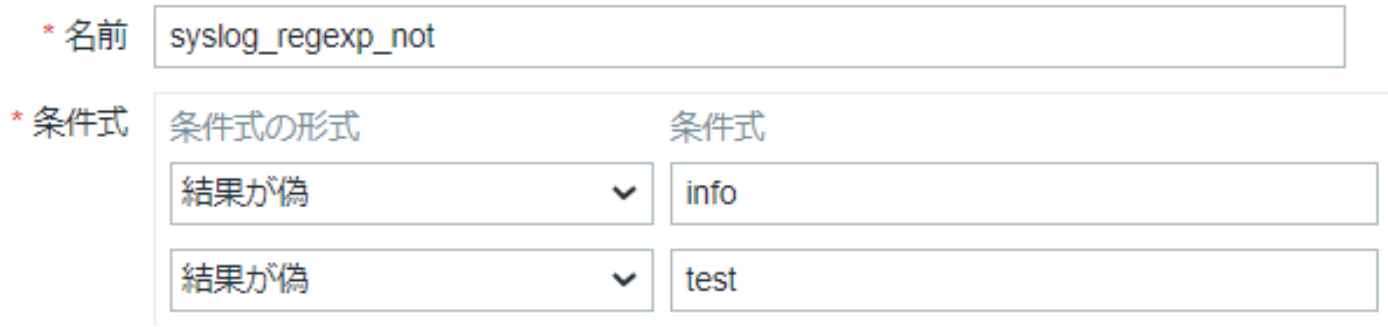
ログ監視のトリガーについて、障害イベント生成モードを複数に設定

⇒トリガーの障害状態に関わらず障害条件を満たした時障害イベントを生成する
⇒エラーログが複数行出力された場合にも漏れなく通知される

2. 監視除外文字列の指定

アイテム：logrt[/var/log/messages.*,@syslog_regexp_not]

正規表現：



⇒正規表現の結果が真となるログデータしか取得しない
⇒監視除外文字列のログは取得せず、監視対象とならない

ログ監視設計

3. 監視文字列の指定

➢ ステップ1：トリガーの条件式に監視文字列を記載

トリガー:

{logrt[/var/log/messages.*].iregexp(error|warn)}=1

※アイテム、アクション、ユーザ等は設定されているものとし以降、説明は省略します

- 監視変更依頼が発生した場合

/var/log/messages

error
warn
crit

を追加

トリガー：

{logrt[/var/log/messages.*].iregexp(error|warn|crit)}=1

トリガーの条件式を変更

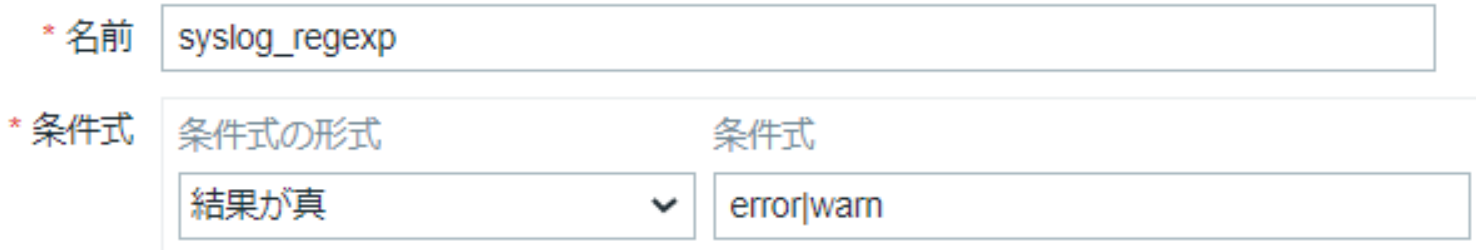
⇒条件式を直接編集するため、オペミスが発生しやすい

ログ監視設計

3. 監視文字列の指定

➢ ステップ2：正規表現に監視文字列を記載

正規表現：



トリガー：

{logrt[/var/log/messages.*].iregexp(@syslog_regexp)}=1

- 監視変更依頼が発生した場合

/var/log/messages

error
warn
crit

を追加

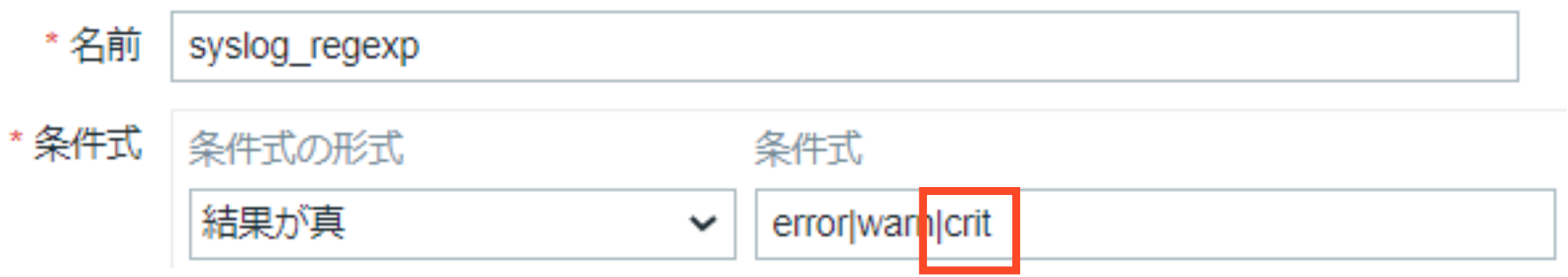
ログ監視設計

3. 監視文字列の指定

➢ ステップ2：正規表現に監視文字列を記載

- 監視変更依頼が発生した場合

正規表現：



赤枠部分を追記

トリガー：

{logrt[/var/log/messages.*].iregexp(@syslog_regexp)}=1

⇒トリガーの条件式は変更不要

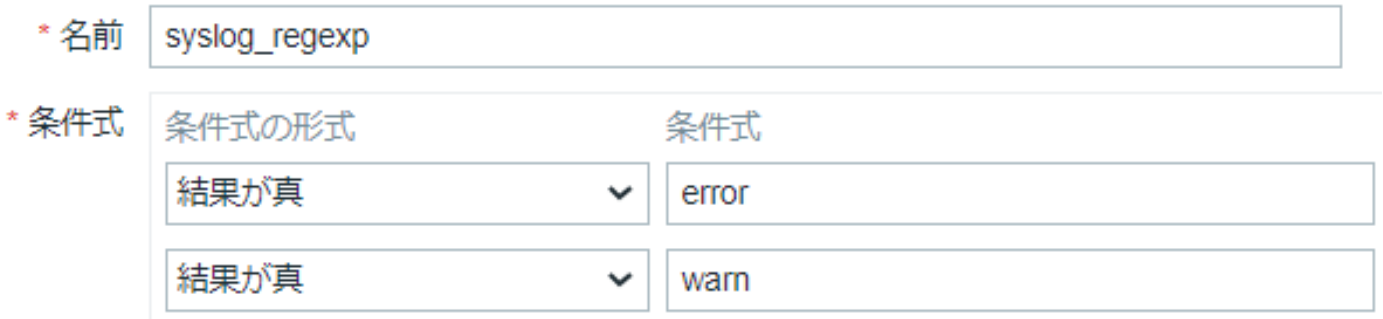
⇒条件式を直接編集するため、オペミスが発生しやすい
⇒条件式の文字数に上限がある(255バイトまで)

ログ監視設計

3. 監視文字列の指定

➢ ステップ3：正規表現の各条件式に監視文字列を記載

正規表現：



トリガー：

{logrt[/var/log/messages.*].iregexp(@syslog_regexp)}=1

⇒監視要件を満たせない

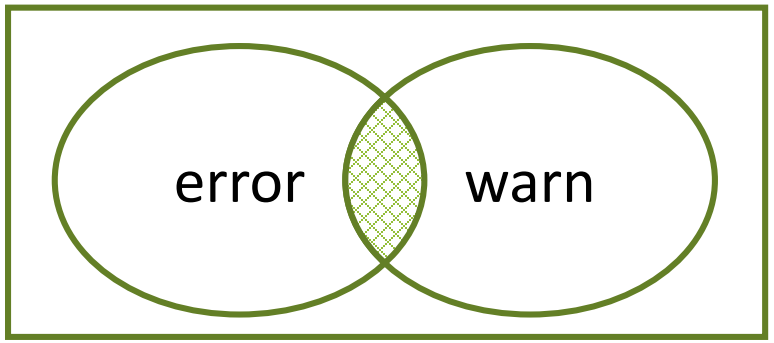
ログ監視設計

3. 監視文字列の指定

➢ ステップ3：正規表現の各条件式に監視文字列を記載

正規表現：

正規表現のベン図



※網掛け部分が真

⇒ error かつ warn を含むログが出力された時障害通知

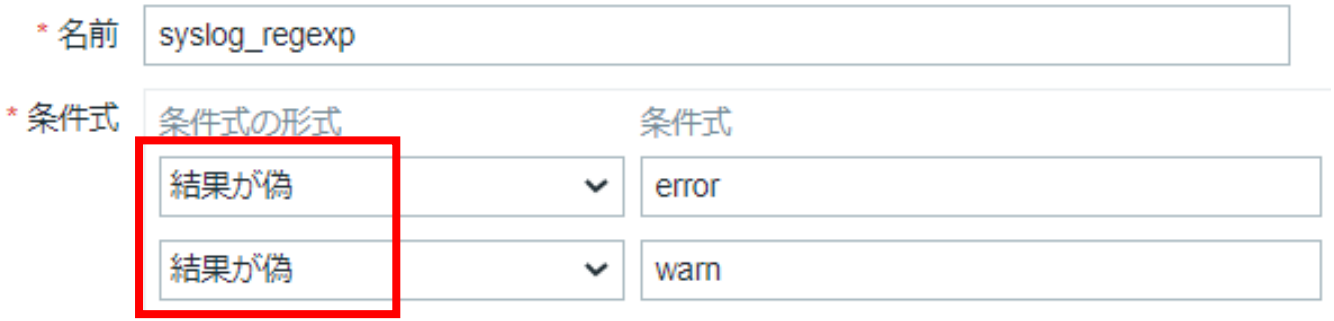
⇒OR条件で判定したいため、AND条件を二重否定する

ログ監視設計

3. 監視文字列の指定

➢ ステップ3：正規表現の各条件式に監視文字列を記載

正規表現：



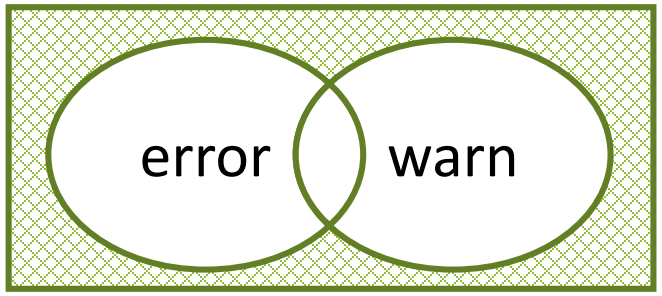
⇒条件式の結果が偽

トリガー：

{logrt[/var/log/messages.*].iregexp(@syslog_regexp)}=0

⇒正規表現の結果が偽

正規表現のベン図



※網掛け部分が真

⇒ error または warn を含むログが出力された時障害通知

ログ監視設計

3. 監視文字列の指定

➢ ステップ3：正規表現の各条件式に監視文字列を記載

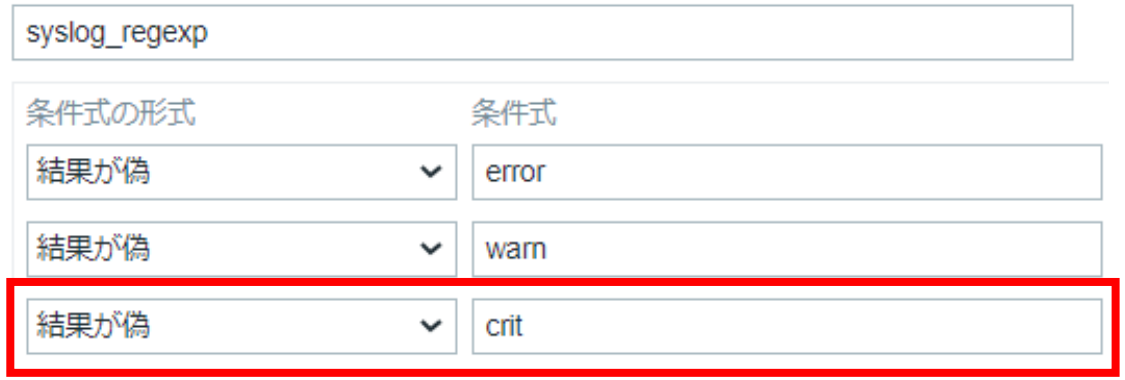
- 監視変更依頼が発生した場合

/var/log/messages

error
warn
crit

を追加

正規表現：



条件式を1行追加

トリガー：

{logrt[/var/log/messages.*].iregexp(@syslog_regexp)}=0

⇒トリガーの条件式は変更不要

⇒既存の条件式は変更せず、追加部分のみ変更する
⇒監視変更(運用作業)が容易

ログ監視設計

4. 大量ログアラートの抑止

トリガー：

{logrt[/var/log/messages.*].count(5m,@syslog_regexp)}>100

⇒過去5分間にエラーログが100件より多く出力された時障害通知
エラーログが100件以下に落ち着いたときは自動で正常状態に復帰する(正常イベントの生成)
障害状態の時に出力されたエラーログについては通知を行わない(障害イベントの単一生成)

ログ監視設計

4. 大量ログアラートの抑止

トリガー：

{logrt[/var/log/messages.*].count(5m,@syslog_regexp)}>100

：過去5分間にエラーログが100件より多く出力された

依存関係

トリガー：

{logrt[/var/log/messages.*].iregexp(@syslog_regexp)}=1

：エラーログが出力された

依存関係：依存先のトリガーが障害状態の時、依存元のトリガーは障害状態にならない

⇒エラーログが100件を超えるまでは通常のログアラート通知を実施する
⇒エラーログが100件を超えた時、大量アラート発生を通知し、以降は通知しない
⇒エラーログが100件以下となった時自動復旧し、通知が再開される

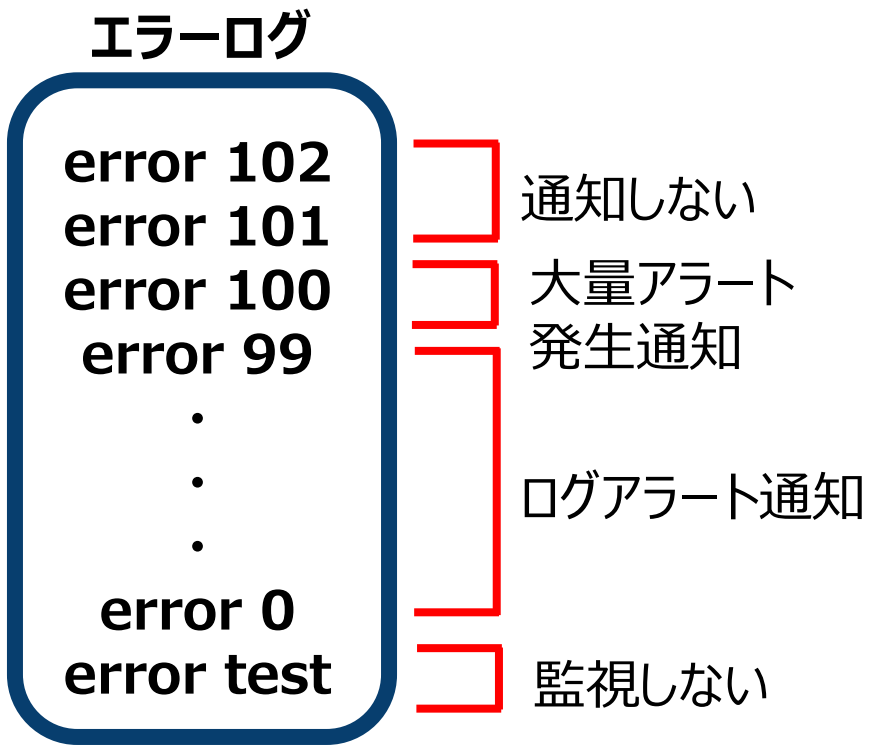
ログ監視設計

- ログ監視設計
  1. 障害イベントの複数設定
  2. 監視除外文字列の指定
  3. 監視文字列の指定
  4. 大量ログアラートの抑止

- ログ監視の動作

監視内容

監視文字列：	error
	warn
監視除外文字列：	info
	test



⇒4点のログ監視設計により、監視要件に沿うログ監視を実現

Appendix.実際の監視設定

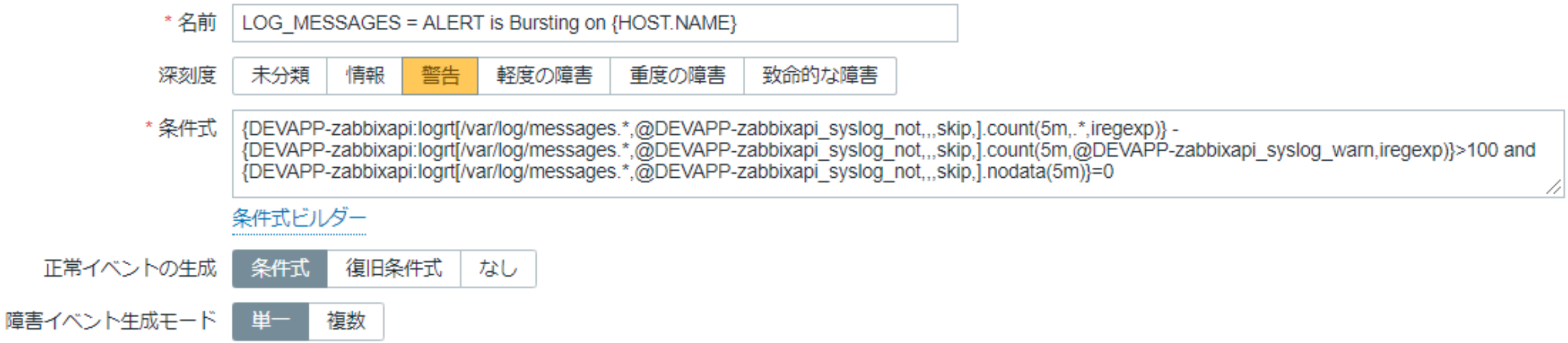
監視設計1から4までを反映させた実際の設定内容：

ログアラート通知トリガー：

Appendix.実際の監視設定

監視設計1から4までを反映させた実際の設定内容：

大量ログアラート発生通知トリガー:

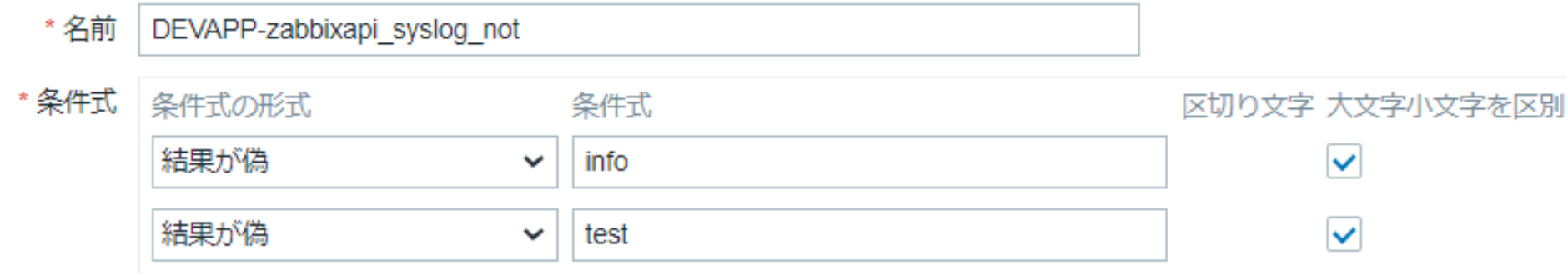


※監視設計3より、@DEVAPP-zabbixapi_syslog_warnは監視文字列に一致しないログをカウントします。
　エラーログの行数を取得するために、ログ全行から監視文字列に一致しないログの行数を減算します。
※nodata関数を利用し、過去5分間にログが出力されていない場合も障害状態から復旧します

Appendix.実際の監視設定

監視設計1から4までを反映させた実際の設定内容：

監視除外文字列の正規表現：



監視文字列の正規表現：

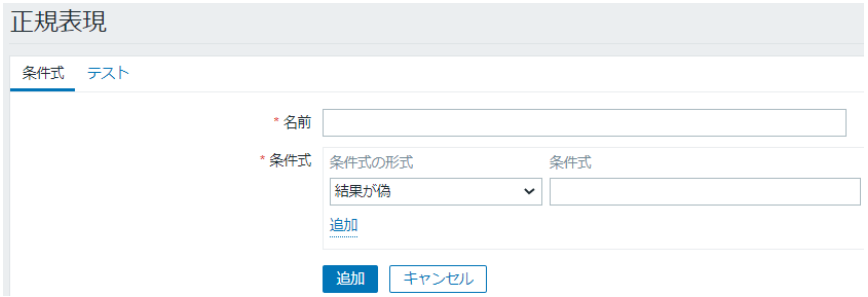
クロージング

- Zabbixに期待すること
  - 正規表現のZabbix API実装

監視設定手順

② スクリプト実行

① 変数ファイルを作成
(監視するリソースとそのしきい値、
監視するログ等を指定)



③ コンソールから正規表現を設定

⇒Zabbix APIで設定したい

⇒③手順をなくしたい

クロージング

- 今後のSAIMONサービス拡大予定
  - Zabbix 5.0対応を検討中

- SAIMON資料請求・お問い合わせ
  - 問い合わせ先：
    カスタマーサービスセンター監視サービス（SAIMON）問い合わせ受付窓口
  - Mail：saimon-sales@sis2.saison.co.jp
  - 営業時間…平日：9時30分～17時

「Speed」+「Quality」⇒「Retention」
～この先も選ばれるサービスへ～