ZABBIX '26

CONFERENCE

LATIN AMERICA

ZABBIX '26
CONFERENCE
LATIN AMERICA

Sneak peek: Correlación de eventos en 8.0

Facundo Vilarnovo
Trainer - GST

Facundo Vilarnovo

GST - Zabbix

marketing.latam@zabbix.com

ZABBIX '26 CONFERENCE LATIN AMERICA

- Zabbix Expert
- Trainer
- Miembro del GST

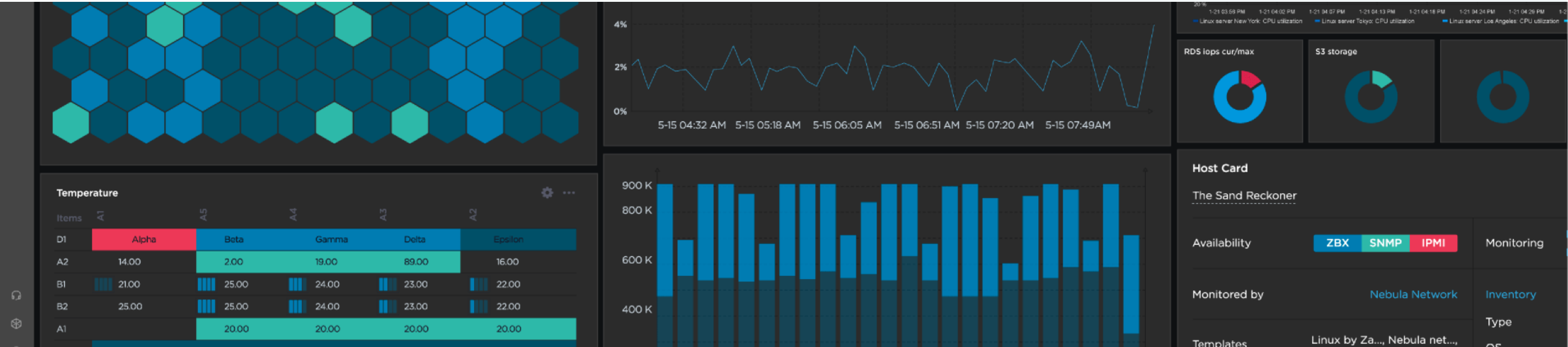
LinkedIn

ZABBIX '26
CONFERENCE
LATIN AMERICA

Contexto

ZABBIX '26 CONFERENCE LATIN AMERICA

Que relacion tiene esta nueva funcionalidad con la correlacion existente

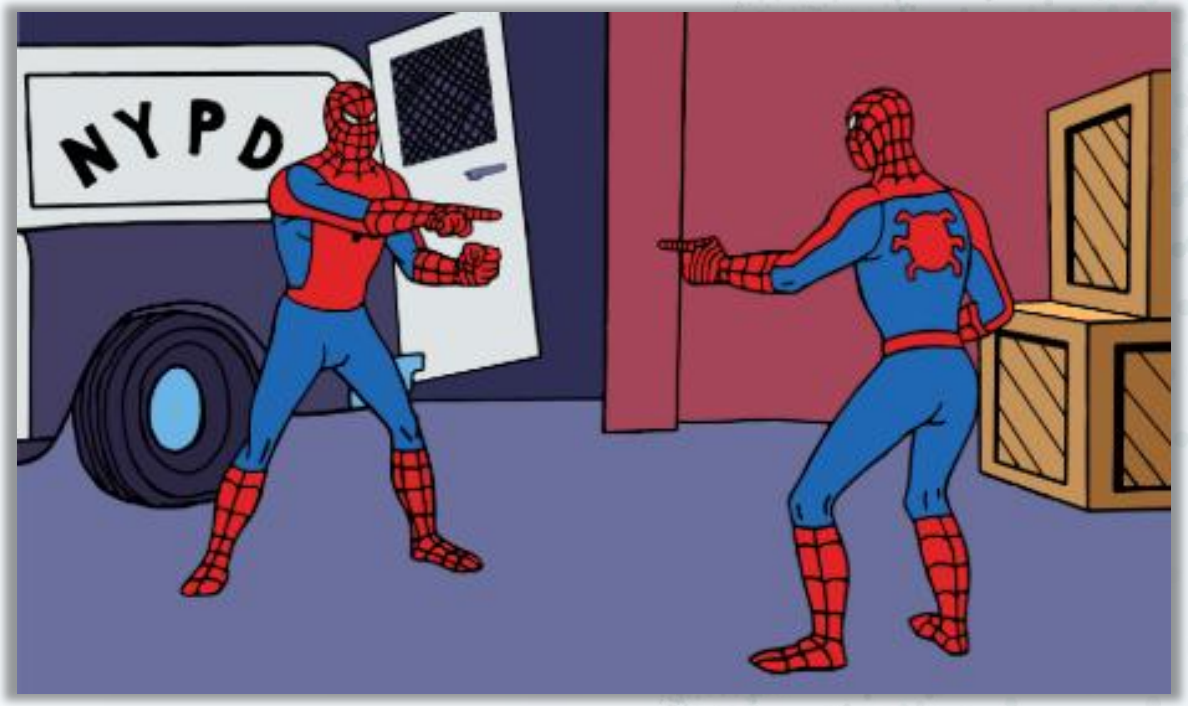


Correlacion actual

ZABBIX '26 CONFERENCE LATIN AMERICA

Actualmente existen 2 tipos de correlación de eventos:

- A nivel de trigger
- A nivel global

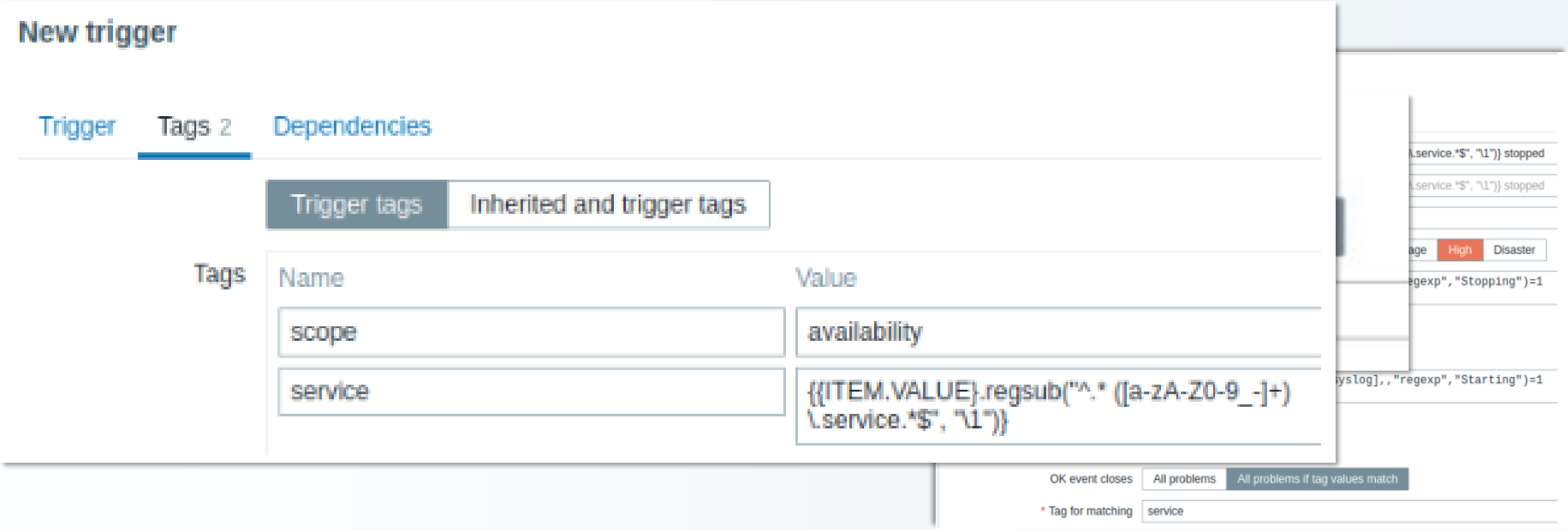


Correlacion basada en triggers

ZABBIX '26 CONFERENCE LATIN AMERICA

Permite relacionar problemas separados reportados por un trigger

- ¿Como funciona?

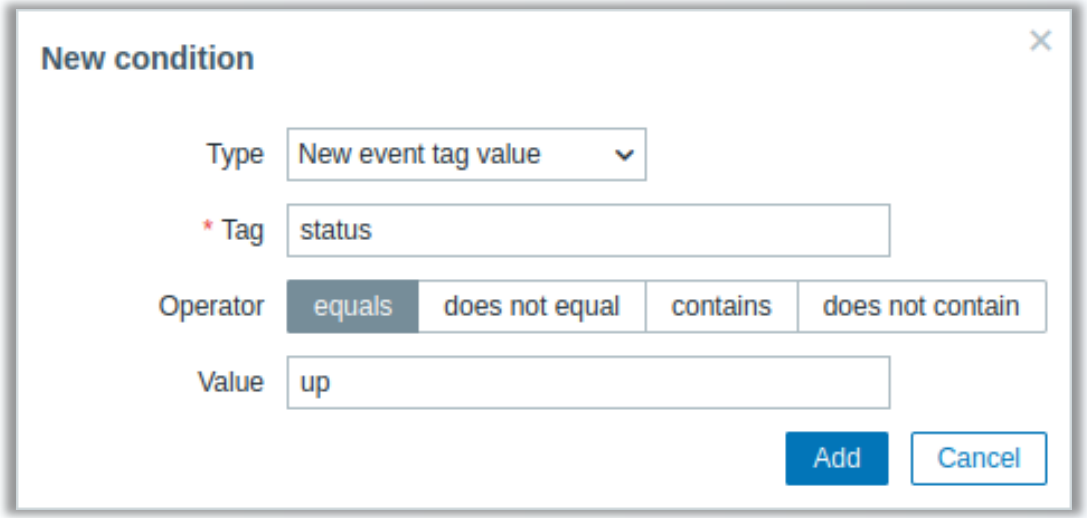


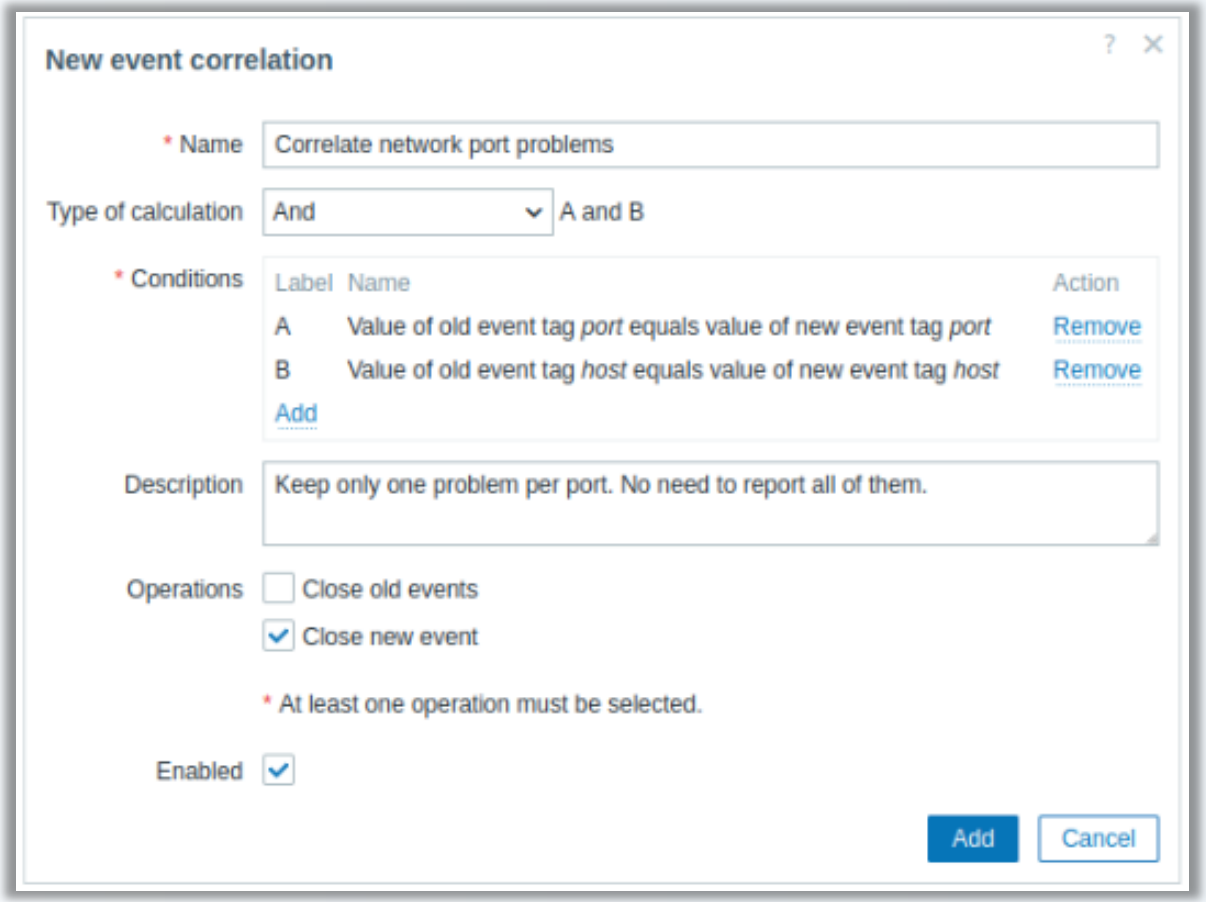
Correlacion global

ZABBIX '26 CONFERENCE LATIN AMERICA

Permite relacionar problemas reportados *distintos* triggers

- Como funciona?
  - Establecemos condiciones y operaciones



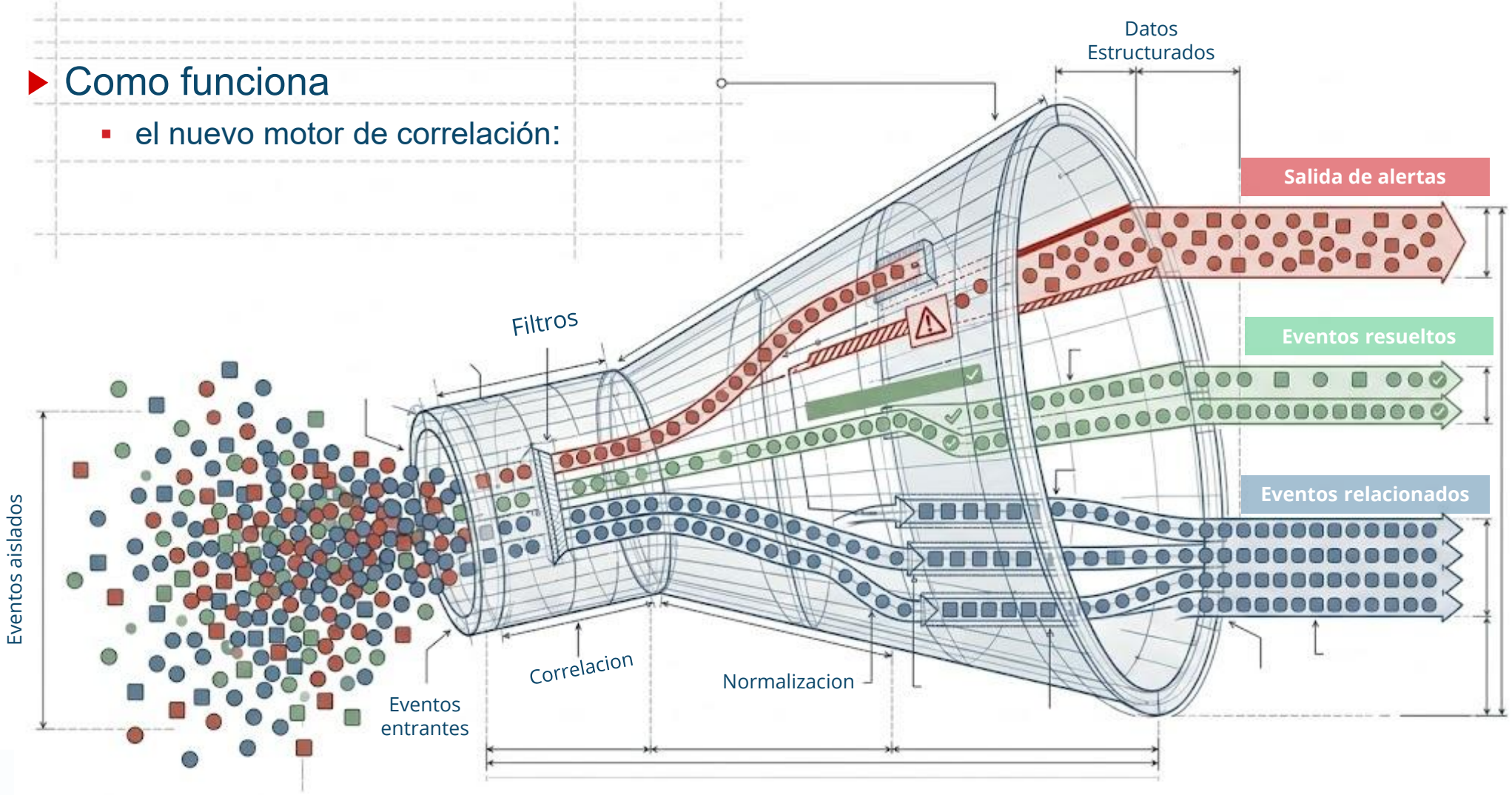


My Elders, my actions speak for themselves.

Complex event processing - CEP

ZABBIX '26 CONFERENCE LATIN AMERICA

- Como funciona
  - el nuevo motor de correlación:




WHAT FACU PROMISED
FEATURES I GOT

Decisio

DEPRECADO

Transicion de

- La correla

ZABBIX '26 CONFERENCE LATIN AMERICA

New complex event processing

* Name: Close events with "error" in name

Type of calculation: Custom expression — A and (B or C) or (D and E and F and G)

Conditions

Label	Name	Action
A	Event name Contains *alert*	Edit Remove
B	Tag name Does not contain *January*	Edit Remove
C	Tag value Contains *:DNS*	Edit Remove
D	Severity Is more than or equal *High*	Edit Remove
E	Host Contains *Mobile*	Edit Remove
F	Host group Equals *backups*	Edit Remove
G	Time period Not in *6-7,00:00-24:00*	Edit Remove

Add

Time window: None | Simple | Cause and symptoms grouping | Tag correlation | Event pattern match

* Duration: 1m

* Capacity: Unlimited | Limited 0

Group by: Host group, Host, Tag

* Event count tag: No | Yes flap-count

Operations

Details	Actions
1: Execute when Tags correlated : Close	Edit Remove
2: Execute when Event pattern matched : Add tag *delegate-server:mirror*	Edit Remove
3: Execute when Tags correlated : Close	Edit Remove
4: Execute when Event evicted : Discard	Edit Remove
5: Execute when Event occured : Set severity *Disaster*	Edit Remove
6: Execute when Event occured : Set tag *algorithm:robin*	Edit Remove
7: Execute when Event occured : Suppress	Edit Remove

Add

Stop processing

* Sort order: 1

Description

Enabled

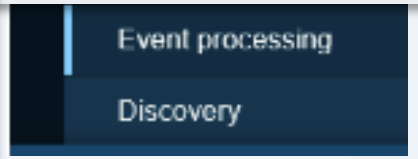
Update | Cancel

Event processing

Create complex event processing | Create event correlation | Filter

Name	Stop after this rule	Sort order	Status
Close events with "error" in name	Enabled	1	Enabled
High severity events	Enabled	2	Enabled
Group cause and symptom events	Disabled	3	Enabled
Correlate tags within 1 hour	Enabled	4	Enabled
Detect event patterns	Disabled	5	Disabled
Correlate host group events	Enabled	6	Enabled
Deduplicate alerts	Enabled	7	Enabled

0 selected | Enable | Disable | Delete



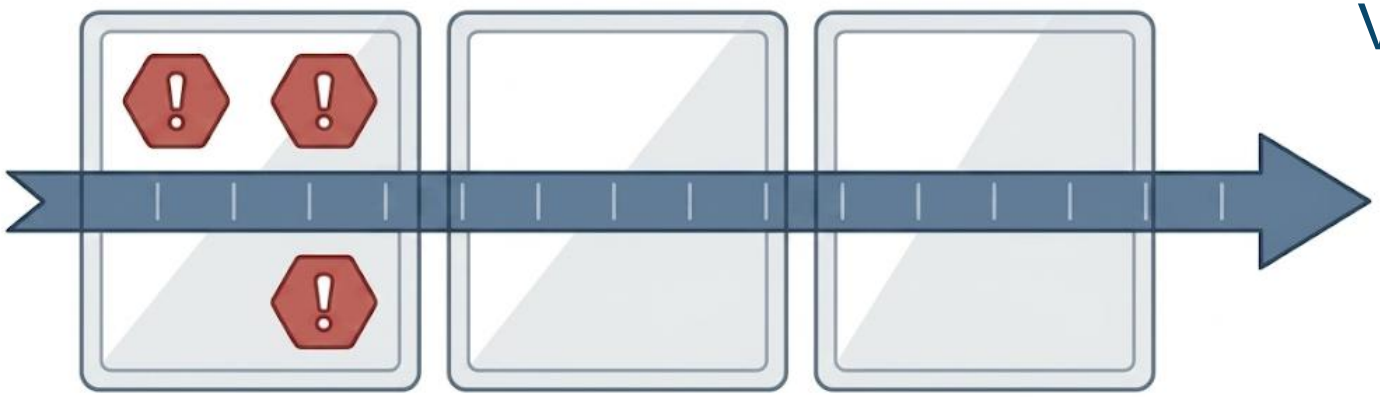
ZABBIX '26
CONFERENCE
LATIN AMERICA

Complex event processing engine

Ventana de tiempo

Ventanas de tiempo

Dos tipos de ventanas de tiempo definen el stream de datos:



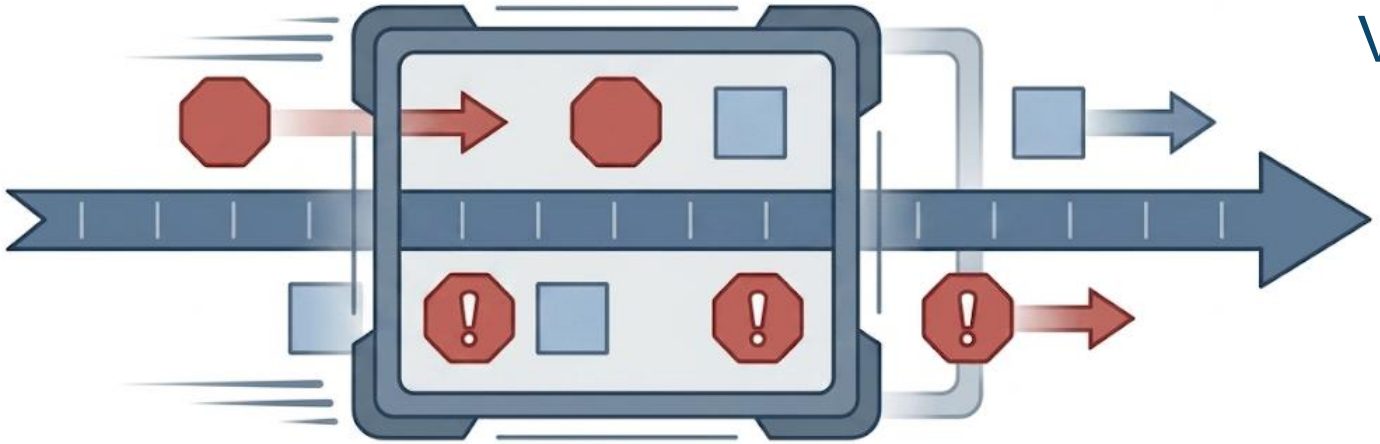
Ventana fija (Fixed/Tumbling):

- Bloques de tiempo estáticos y consecutivos

Un evento pertenece a una sola ventana.

Al agotarse la duración, la ventana se cierra

Ideal para agrupar problemas.



Ventana deslizante (Sliding):

- Marco de duración constante que avanza:

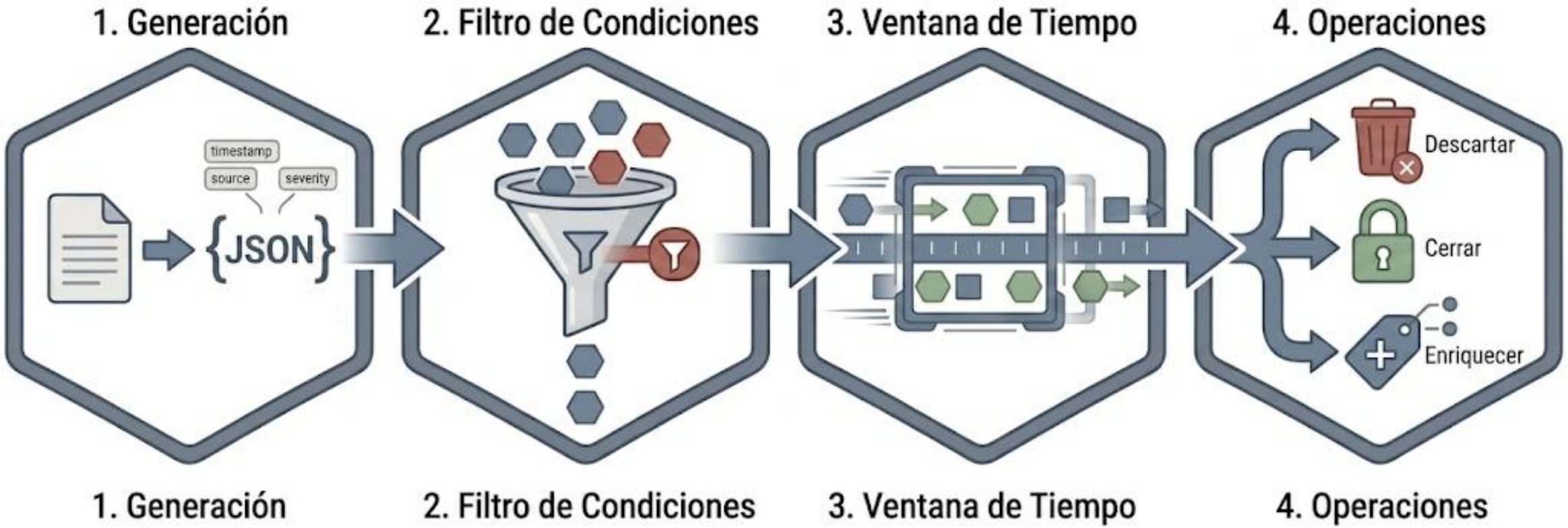
Un mismo evento es analizado por multiples marcos superpuestos.

Ideal para patrones continuos.

Pipeline de procesamiento:

ZABBIX '26 CONFERENCE LATIN AMERICA

El servidor trabaja con eventos estructurados y los envia a CEP:



Matriz de decisión: Tipos de Ventana

ZABBIX '26 CONFERENCE LATIN AMERICA

Tipo de Calculo	Tipo de Ventana	Lógica Principal	Caso de uso ideal
Simple	Deslizante/Sliding	Expulsión de eventos por limite de tiempo o capacidad	Cierre diferido y limpieza de eventos
Agrupación (Causa/síntoma)	Fija/Fixed	El primer evento es la 'Causa'; los eventos subsecuentes se agrupan como 'Síntomas'	Reducción de ruido y de-duplicación.
Correlación de tags	Deslizante/Sliding	Mapea eventos pasados y actuales cruzando valores de tags	Correlación clásica
Coincidencia de patrones	Deslizante/Sliding	Ejecuta JavaScript buscando secuencias lógicas	Prevención de fraude y secuencias criticas

Group by (Opcional)

All (default) | Host group | Host | Tag - Puede contener combinaciones (Ej. "Host , Tag")

Creacion de una regla

ZABBIX '26 CONFERENCE LATIN AMERICA

Primero debemos establecer las condiciones:

Las condiciones actúan como un filtro, determinando que flujo de eventos son considerados (por nombre, tag, severidad, host, etc)

New complex event processing

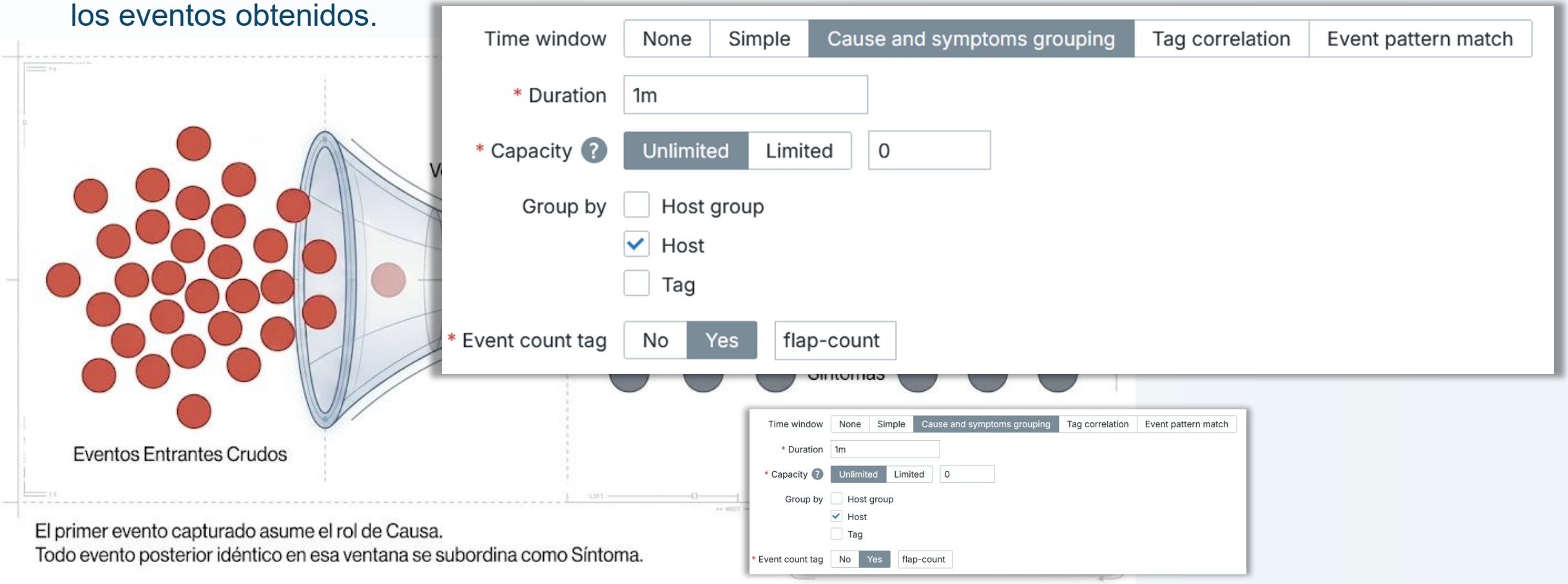
* Name	Close events with "error" in name		
Type of calculation	Custom expression	A and (B or C) or (D and E and F and G)	
Conditions	Label	Name	Action
	A	Event name Contains *alert*	Edit Remove
	B	Tag name Does not contain *January*	Edit Remove
	C	Tag value Contains *:DNS*	Edit Remove
	D	Severity Is more than or equal *High*	Edit Remove
	E	Host Contains *Mobile*	Edit Remove
	F	Host group Equals *backups*	Edit Remove
	G	Time period Not in *6-7,00:00-24:00*	Edit Remove
	Add		

Creacion de una regla - Cause & Symp

ZABBIX '26 CONFERENCE LATIN AMERICA

El segundo paso es definir la ventana de tiempo

La ventana establece el criterio sobre los eventos obtenidos.

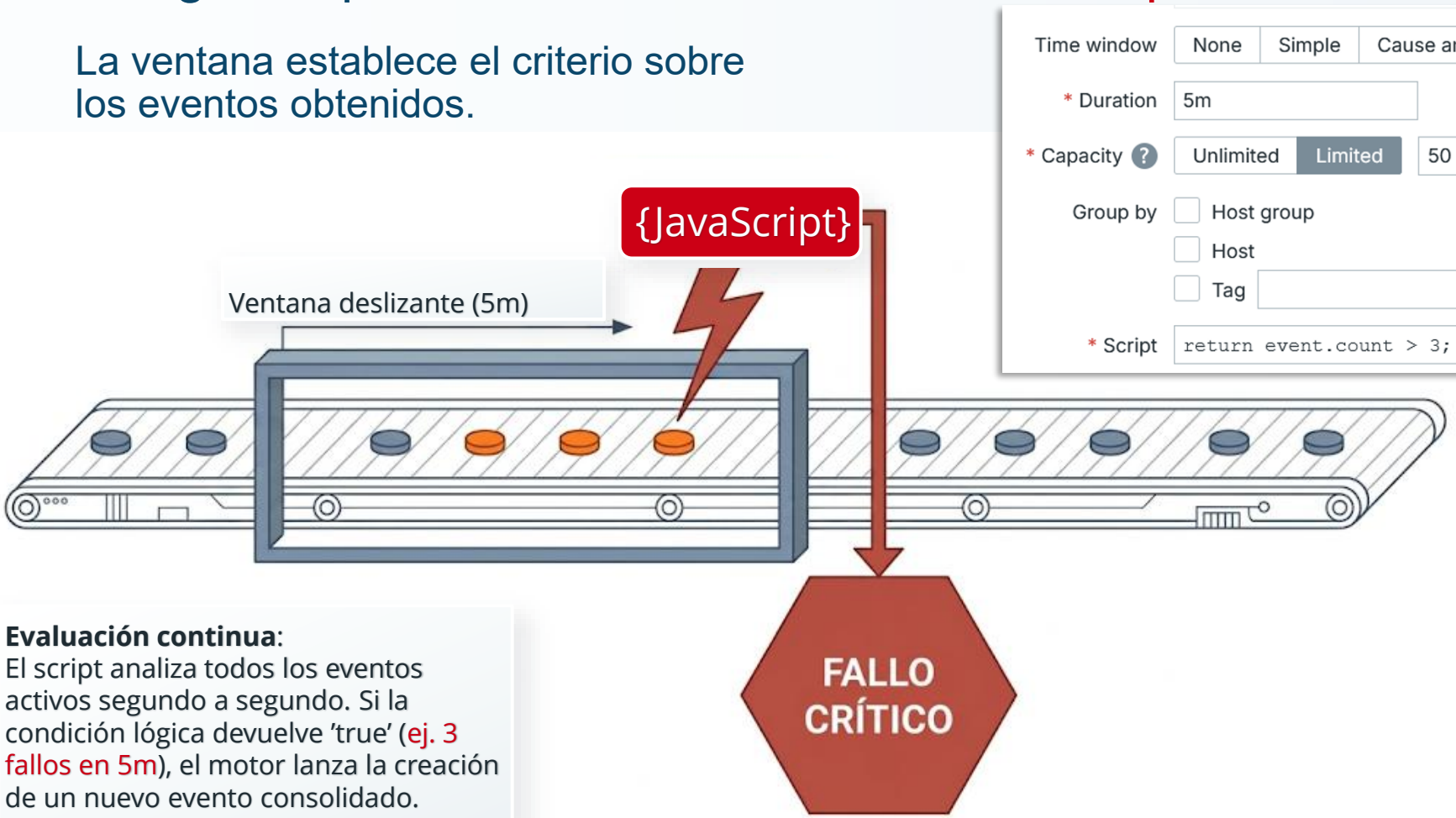


Creacion de una regla - Event pattern

ZABBIX '26 CONFERENCE LATIN AMERICA

El segundo paso es definir la ventana de tiempo

La ventana establece el criterio sobre los eventos obtenidos.



Time window	None	Simple	Cause and symptoms grouping	Tag correlation	Event pattern match
* Duration	5m				
* Capacity ?	Unlimited	Limited	50		
Group by	Host group				
	Host				
	Tag				
* Script	`return event.count > 3;`				

Evaluación continua:
El script analiza todos los eventos activos segundo a segundo. Si la condición lógica devuelve 'true' (ej. 3 fallos en 5m), el motor lanza la creación de un nuevo evento consolidado.

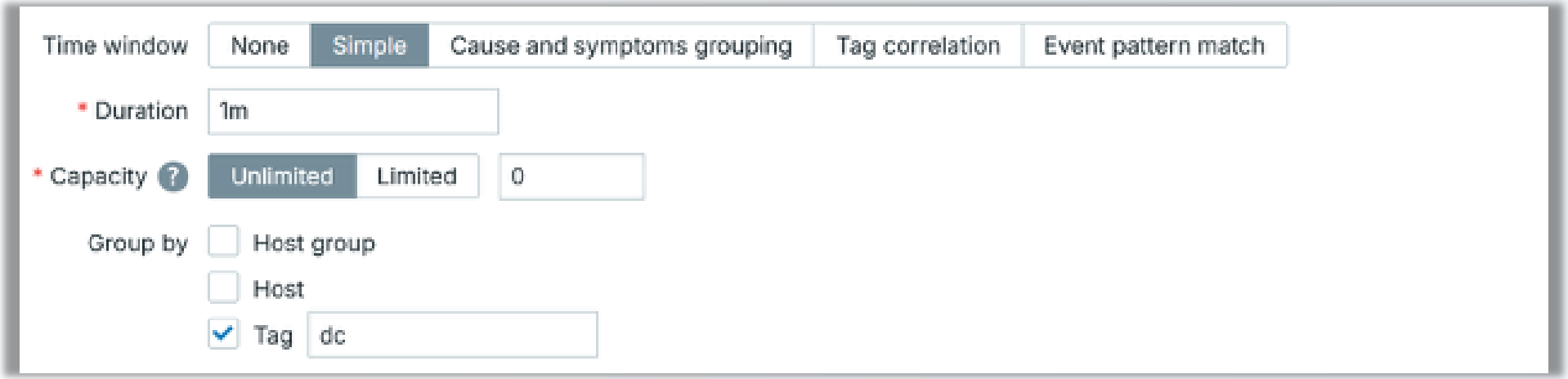
Creacion de una regla - Simple

ZABBIX '26 CONFERENCE LATIN AMERICA

El segundo paso es definir la ventana de tiempo

La ventana establece el criterio sobre los eventos obtenidos.

Sliding con Group by: Agrupacion por datacenter



Duracion 1m | Capacity: Unlimited | Group by: Tag “dc”. Si la severidad es >= Information, se agrupa por tag dc y se ejecuta: Set severity disaster + Add tag processed:true

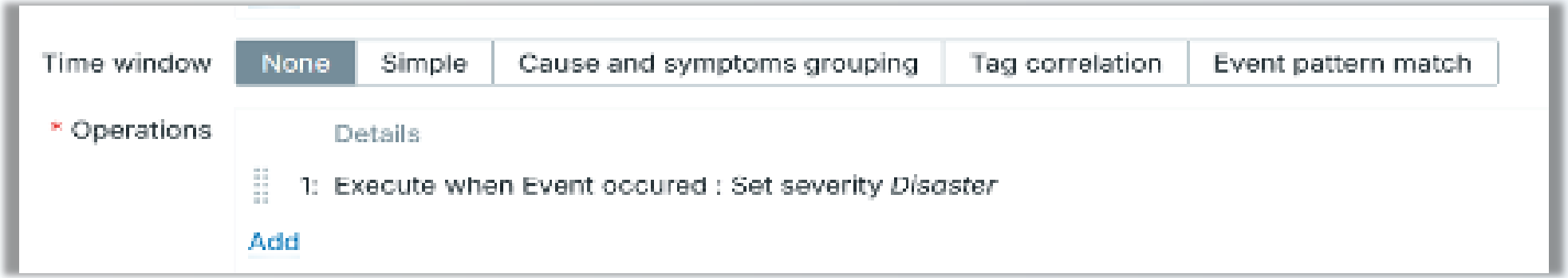
Creacion de una regla - None

ZABBIX '26 CONFERENCE LATIN AMERICA

El segundo paso es definir la ventana de tiempo

La ventana establece el criterio sobre los eventos obtenidos.

Single-event rule: cada evento se evalua individualmente



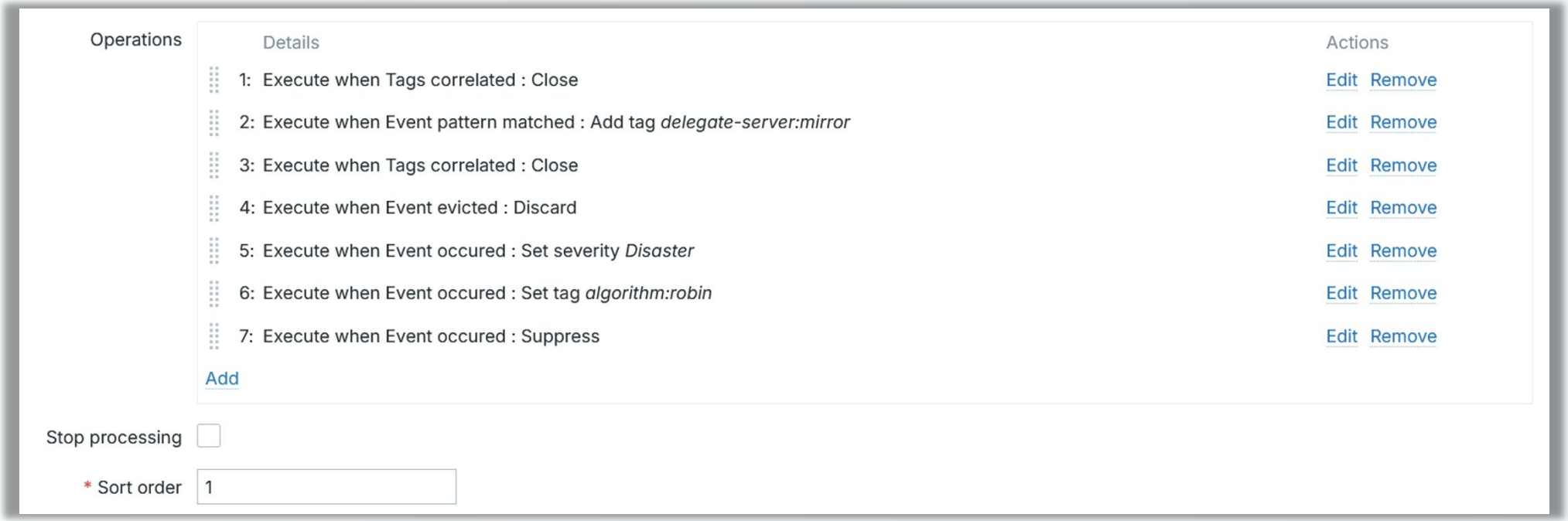
Time window: None - Sin ventana de tiempo. La condición Severity >= Information se evalua evento por evento.

Creacion de una regla

ZABBIX '26 CONFERENCE LATIN AMERICA

El tercer y ultimo paso son las operaciones

- Las operaciones definen las transacciones a realizar sobre los eventos
- Definiremos si estas operaciones detienen el procesamiento
- Establecemos el orden o posición de nuestra regla



ZABBIX '26
CONFERENCE
LATIN AMERICA

Complex event processing engine

12+ Operaciones sobre eventos

Operaciones sobre eventos y tags

ZABBIX '26 CONFERENCE LATIN AMERICA

Eventos:

Operación	Restricción	Descripción
Event name set	Excepto pattern matched	Nuevo nombre para el evento
Event close	--	Cierra el evento
Event discard	Excepto por tags correlated	Descarta el evento
Severity set	--	Establece severidad
Severity increase	--	Aumenta +1
Severity decrease	--	Reduce -1
Event suppress	--	Suprime por tiempo
Copy first as new	Pattern match, reemplazo	Copia el primer evento
Copy last as new	Pattern match, reemplazo	Copia el ultimo evento

Tags:

Operación	Descripción
Tag add	Agrega nuevo tag si el nombre no existe
Tag set	Agrega o actualiza si ya existe
Tag value set	Actualiza valor del tag existente
Tag value increase	Valor numérico +1
Tag value decrease	Valor numérico -1
Tag rename	Renombra
Tag remove	Elimina dicho tag

12+ Operaciones donde la correlación global solo tenia 2 (Close old/Close new)

Casos de uso

ZABBIX '26 CONFERENCE LATIN AMERICA

El playbook de CEP: Aplicaciones en el mundo real:

Como resuelve problemas históricos mediante reglas predefinidas.

Flujo simple
Enriquecimiento y Normalización.
Ej: Agregar dinámicamente tags “env:prod” u ocultar datos sensibles antes del almacenamiento

Flujo temporal
Cierre diferido automático.
Ej. Purgar y cerrar silenciosamente alertas de baja prioridad que superen los 14 dias

Agrupación Estructural
Deduplicacion y reducción de ruido.
Ej: Colapsar 100 eventos intermitentes en un solo evento raiz

Patrones Avanzados
Detección de secuencias y vacíos.
Ej. Alertar de fraude basado en ráfagas de eventos o notificar cuando un “heartbeat” desaparece

Arquitectura, Desacoplamiento y Resiliencia

ZABBIX '26 CONFERENCE LATIN AMERICA

Desacoplamiento Total
CEP opera como un proceso independiente, lo que mejora el rendimiento del servidor

Protección Estricta
Mecanismos nativos previene bucles circulares, garantizando la estabilidad del backend

Resiliencia de Estado
Tolerancia absoluta a reinicios planificados y caídas imprevistas; las ventanas de tiempo no pierden eventos en memoria

ZABBIX '26
CONFERENCE
LATIN AMERICA

Gracias!

Facundo Vilarnovo

Trainer - GST