

**ZABBIX '24**

CONFERENCE

LATIN AMERICA

JUNE, 07-08, 2024. SÃO PAULO, BRAZIL

ZABBIX '24

CONFERENCE

LATIN AMERICA

# Disminución del MTTR en Telefónica Colombia utilizando Zabbix



\*\*\*Este documento está clasificado como PÚBLICO por TELEFÓNICA.  
\*\*\*This document is classified as PUBLIC by TELEFÓNICA.

# Carlos Ortega



**+15 Años** En sistemas de monitoreo

**+10 Años** En sistemas Zabbix



carlos.ortega@imagunet.com



[www.linkedin.com/in/carlos-ortega-guerrero](https://www.linkedin.com/in/carlos-ortega-guerrero)

# Jairo Fernando Díaz Toro



**+19 Años** En Telefónica

**5 Años** con Zabbix en nuestra operación



**Jairo Fernando Díaz Toro**  
Product Owner Senior AIOPS TI  
jairof.diaz@telefonica.com |  
Móvil +57 3153117041



[jairof.diaz@telefonica.com](mailto:jairof.diaz@telefonica.com)



<https://www.linkedin.com/in/jairo-fernando-diaz-toro>

# ¿Quiénes somos?

Imagunet es una empresa apasionada por el software Open Source, utilizamos tecnologías basadas en este concepto para ofrecer servicios y soluciones profesionales, confiables, robustas, escalables y costo-eficientes.

Somos el resultado de varios años de experiencia, con más de:



**+100**

Clientes

**+200**

Proyectos ejecutados con éxito a nivel Latinoamérica



# ¿Qué hacemos?



## SERVICIOS ABIERTOS EN LA NUBE

Su Infraestructura de TI como Servicio Web, de la mano de AWS usando lo mejor del mundo OpenSource (Kafka – base, Keycloak, etc.).

## MONITOREO ZABBIX

Monitoreo predictivo de su negocio en tiempo real, por medio de Zabbix, Grafana.

## ITSM Y AUTOMATIZACIÓN - GLPI

Seguimiento del estado de infraestructura, licencias, incidentes de forma automática.

## SEGURIDAD INTEGRAL

Visibilidad y control con una herramienta SIEM, XDR y EDP completa como lo es Wazuh.

## MARIADB BASES DE DATOS

Ofrecemos diferentes soluciones tecnológicas, como bases de datos, soportados por algunos de los mejores socios del mercado como MariaDB.

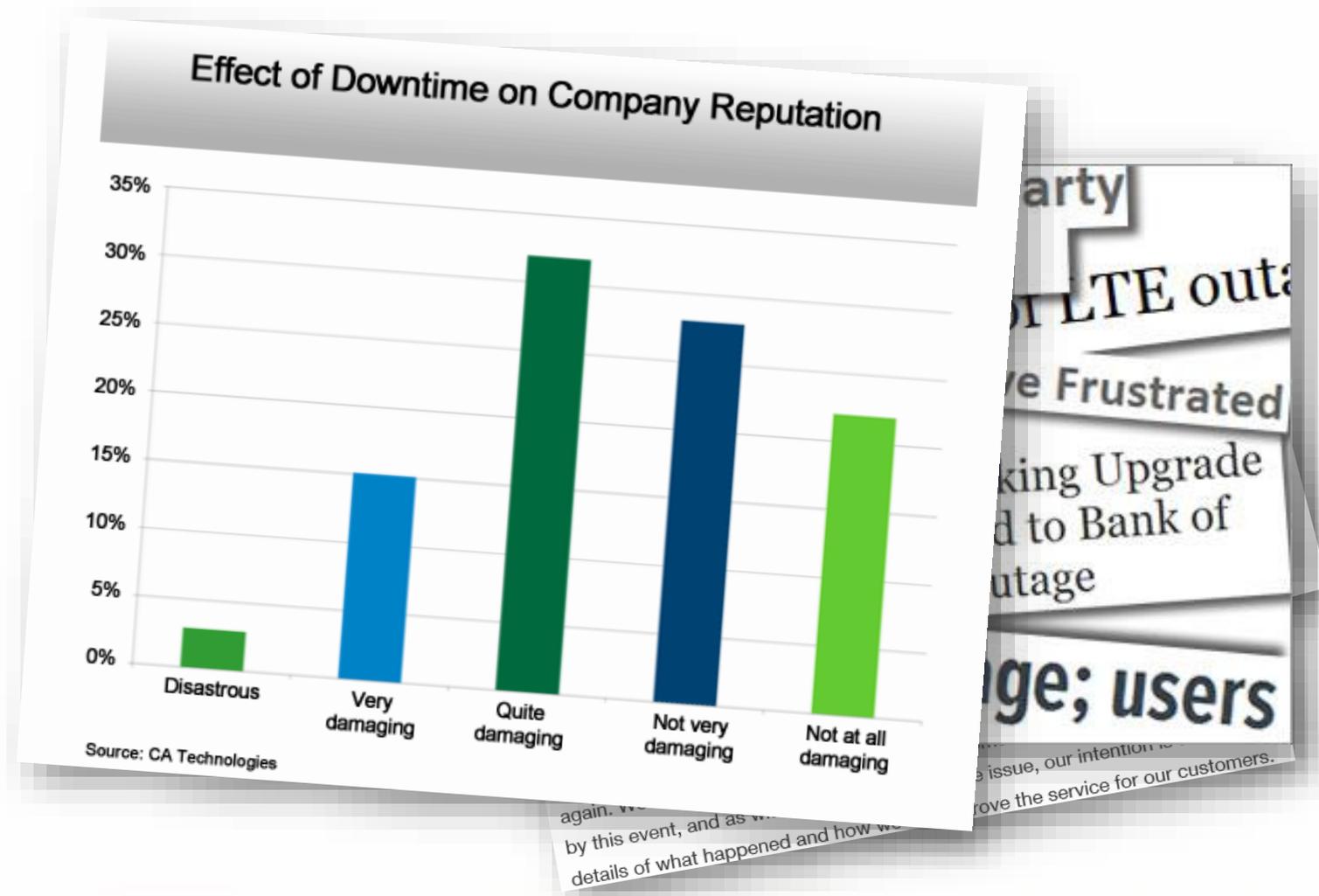
## INTERNET DE LAS COSAS

Gran variedad de sensores para monitorear absolutamente todo con múltiples tecnologías.



# Conceptos básicos

# Pérdida ante una falla



# Mantenimientos

## Reactivo

Solución a problemas  
luego de ocurridos



## Preventivo

Actividades planificadas  
para evitar problemas



## Proactivo

Anticipar y prevenir  
problemas mediante  
tecnologías avanzadas



# ¿Que es MTTR?

El MTTR (tiempo medio de reparación) es una métrica utilizada para medir el tiempo promedio que se tarda en reparar un sistema o equipo después de que haya fallado.

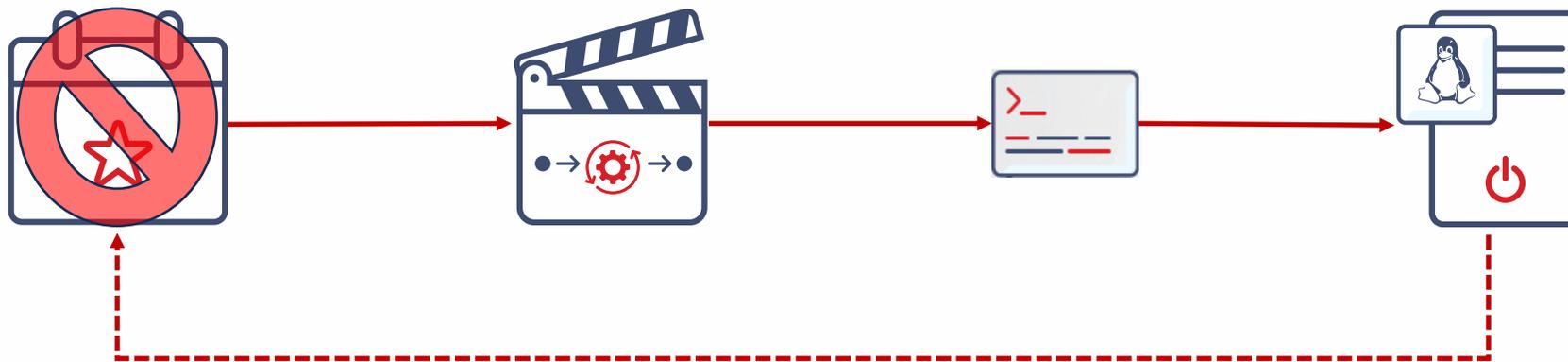
Reducir el MTTR implica mejorar la eficiencia en las reparaciones y minimizar el tiempo de inactividad.

$$MTTR = \frac{\textit{Tiempo total de fallas}}{\textit{Cantidad de fallas}}$$

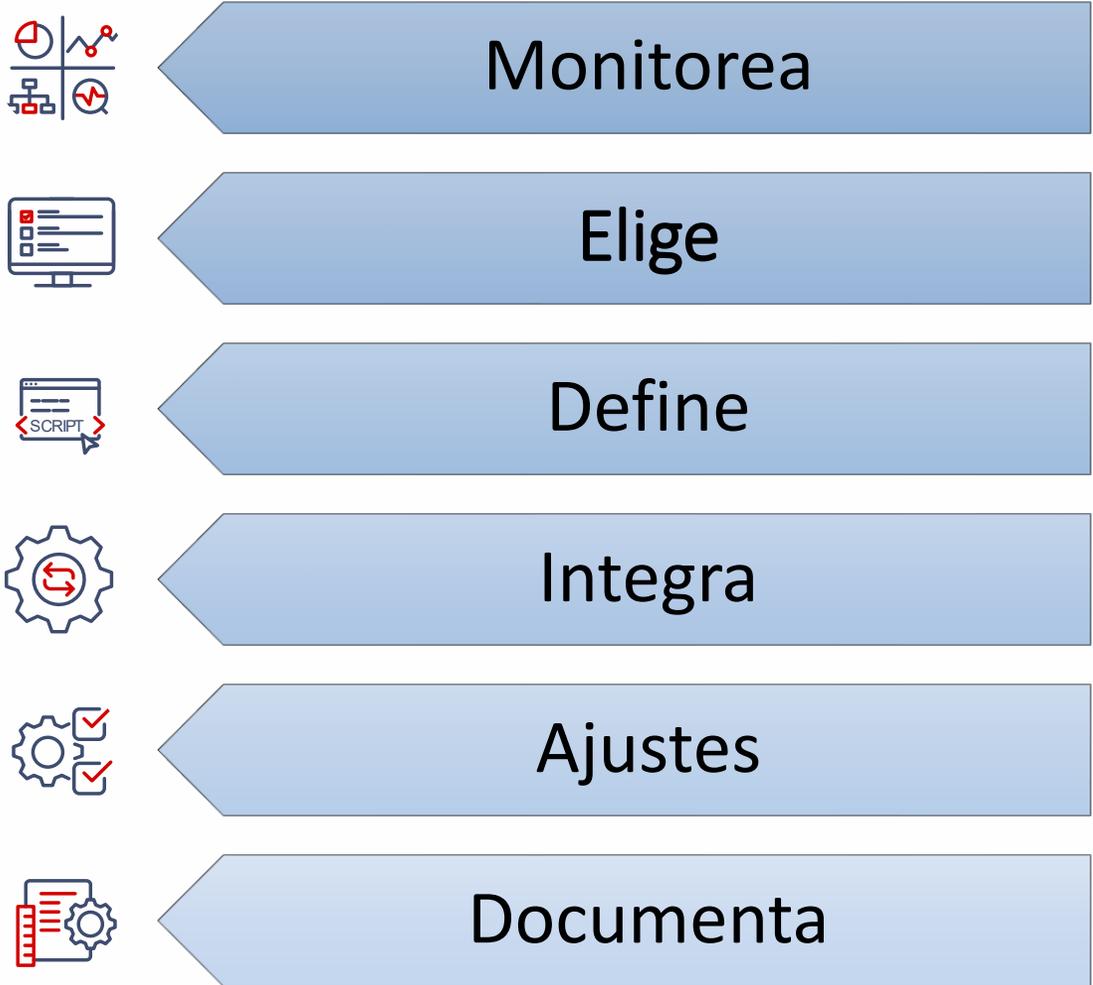
# Autoremediación

Se refiere a la capacidad de un sistema para identificar y resolver problemas automáticamente sin intervención humana.

- Eficiencia y Tiempo
- Reducción de errores humanos
- Escalabilidad
- Reducción de costos



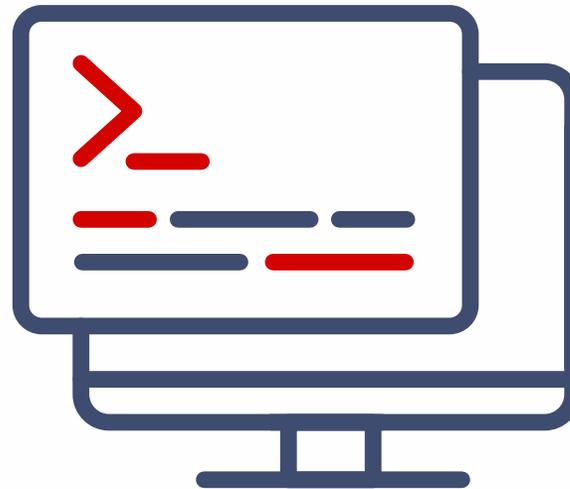
# Paso a Paso



# Scripts (antes Global Scripts)

Scripts o set de comandos ejecutados por los componentes de Zabbix para:

- Integración con terceros.
- Rutinas de mantenimiento.
- Obtención de data.
- **Autoremediación.**



# Parámetros importantes

Menú de Host: Dashboard, Problems, Latest data, Maps, etc

Menu de Eventos: Dashboard, Problems

Actions: **Operaciones automaticas**

## Script

\* Name

Scope  Action operation  Manual host action  Manual event action

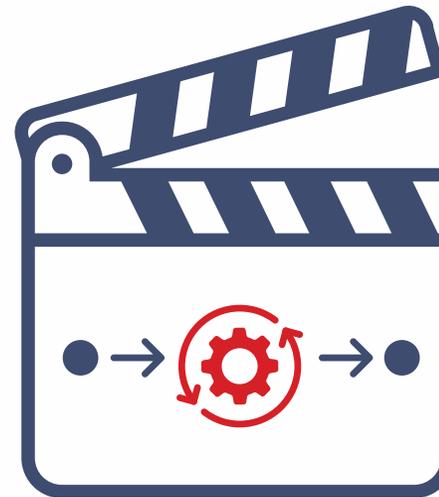
Type  Webhook  Script  SSH  Telnet  IPMI

Execute on  Zabbix agent  Zabbix proxy or server  Zabbix server 

# Actions

Ejecutar una acción como respuesta a un evento:

- Enviar un mensaje.
- Actualizar estado de un evento.
- **Enviar un comando.**



# Parámetros importantes

Conditions: ¿Qué lo dispara?

Step: ¿Cuándo lo dispara?

Operation: ¿**Qué dispara?**

Action Operations 1

\* Name Remediation

Type of calculation And/Or A and B

Conditions

Label	Name
A	Host group equals Zabbix servers
B	Trigger equals Zabbix server 7.0: Linux: High CPU utilization

Action Operations 1

\* Default operation step duration 1h

Operations	Steps	Details	Start in
	1	Run script "Remote restart" on current host	Immediately

# Primeros pasos de Autoremediación

- Limpieza de filesystem
- Reinicio procesos
- Terminar queries colgados en DB
- Autoescalamiento de webservices o contenedores
- Reinicio de puertos, si hay muchos drop de paquetes
- Activación de actuadores por sensores de IOT



Zabbix Demo: History [refreshed] x +

demo.imagnet.com/zabbix/history.php?action=sh... Reinicia para actualizar

WhatsApp Traducción zabbix

Last 1 year Previous year This month so far Last 6 hours  
Last 2 years This year Last 12 hours  
This year so far Last 1 day

Zabbix Server Demo: Used disk space on / (%)

53.691 %

I-DEMO-ZBX-SRV-00 - Interno x +

stage.imagnet.com:444/?viewmode=12&gotonode=iWuwt6FKGOT3UmoNRFgEuAyRd86gFzqzf9Vy2tCjuQX8

WhatsApp Traducción zabbix

IMAGUNET

General Terminal Archivos Eventos Detalles Consola

Terminal - I-DEMO-ZBX-SRV-00 - Interno

Desconectar Conectado - root@I-DEMO-ZBX-SRV-00: /tmp/autoreem Acciones

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/nvme0n1p1  54G   29G   25G  55% /
Filesystem      Size  Used Avail Use% Mounted on
/dev/nvme0n1p1  54G   30G   25G  55% /
^C
root@I-DEMO-ZBX-SRV-00:/tmp/autoreem#
```

Ctrl-C Ctrl-X ESC

15:32:41 Ctrl-A (1) Enviar

Telegram Web x +

WhatsApp Traducción zabbix

Imagu Demo Alerts 10 members

Last Value: 0.2003457685417393 10:58

ImaguAlerts  
Resolved: Zabbix DB 02  
Node sending Flow Controls to Cluster

Severity: Average  
Duration: 15m 5s 11:11

ImaguAlerts  
Problem: Web Page 2021  
High CPU utilization (over 95% in service php-fpm)

Severity: High  
Time: 2023.11.16 11:52:51

Message

Zabbix Demo: Problems

demo.imagnet.com/zabbix/zabbix.php?show=1&name=&inven...

WhatsApp Traducción zabbix

### Problems

Time	Severity	Recovery time	Status	Info	Host	Problem
23:05:52	Average		PROBLEM		I-OFIC-LAP-PAO-00	High Memory Utilization (over 90%)
23:05:19	Warning		PROBLEM		I-OFIC-LAP-PAO-00	The Memory Pages/sec is too high (over 1000 for 15m)
23:00						
22:31:15	Average		PROBLEM		Ocamonte	Disponibilidad por debajo del 95% en Ocamonte
22:23:38	Average		PROBLEM		Iza	Disponibilidad por debajo del 95% en Iza
22:13:45	Average		PROBLEM		I-OFIC-LAP-NED-00	Zabbix agent is not available (or nodata for 30m)

Telegram Web

web.telegram.org/k/...

WhatsApp Traducción zabbix

Imagu Demo Alerts  
10 members

Node sending Flow Controls to Cluster

Severity: Average  
Duration: 15m 2s  
10:23

ImaguAlerts  
Problem: Imagu-TelegramBot  
Bad Gateway

Severity: Warning  
Time: 2023.11.18 20:10:43

Last Value: 2023-11-18 20:10:18,634 - telegram.ext.updater - ERROR - Error while getting Updates: Bad Gateway  
20:12

Message

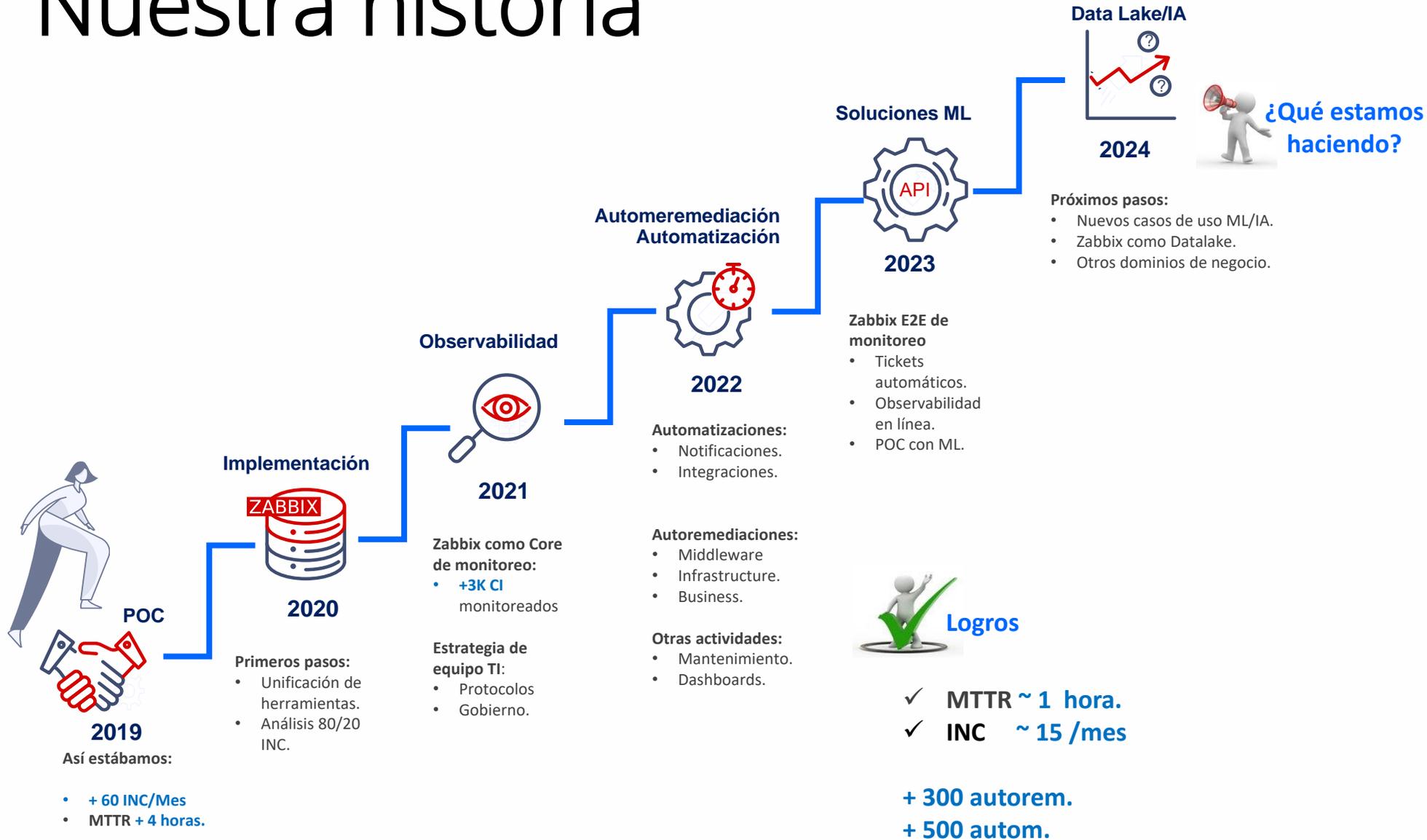
Desconectar Conectado - root@I-DEMO-ZBX-SRV-00: /usr/local/mesh\_services/meshagent

```
root@I-DEMO-ZBX-SRV-00:/usr/local/mesh_services/meshagent#
```

00:04:21 Ctrl-A (1) Enviar

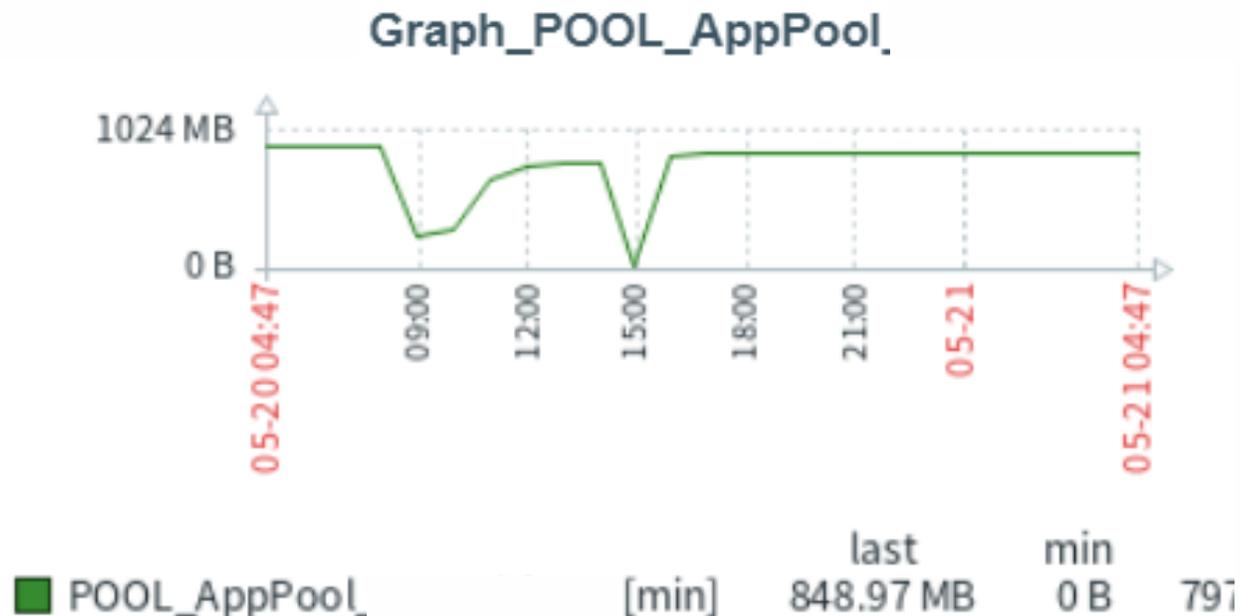
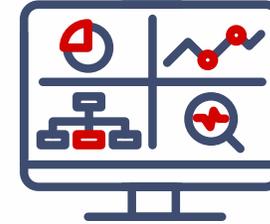
# Caso de Uso: Telefónica Colombia

# Nuestra historia



# Caso práctico - Necesidad

INC reiterados por consumo de memoria app\_pool



2022:

+3 INC críticos diarios por consumo de memoria de los app\_pool.

# Caso práctico - Monitor



## Autoremediación IIS-Trigger

### Item prototypes

All templates / TMC Template Module IIS Pool Me... Discovery list / Work Process Pool Win New Relea... Item prototypes 1 Trigger prototypes 2 Graph prototypes 1

<input type="checkbox"/>	Name ▲	Key	Interval	History	Trends
<input type="checkbox"/>	... POOL_{#NAME_POOL}	system.run[%windir%\system32\inetsrv\appcmd list wp && echo ! && powershell -c "Get-Process -name \"w3wp!\" && echo ! && echo {#NAME_POOL}]	2m	90d	365d

### JavaScript

```
function (value) {  
  1 var pool = '{#NAME_POOL}'.trim();  
  2 var consumo = 0;  
  3  
  4 if (value === '') {  
  5   return consumo;  
  6 }  
  7  
  8 var valueArr = value.split("!");  
  9  
 10 var wpArr = valueArr[0].split("\n");  
 11 var processArr = valueArr[1].split("\n");  
 12 var arr = [];  
 13  
 14 var listWp = [];  
 15 var listProcess = [];  
 16  
 17 // LISTA DE PROCESOS  
 18 wpArr.forEach(function (e) {  
 19
```

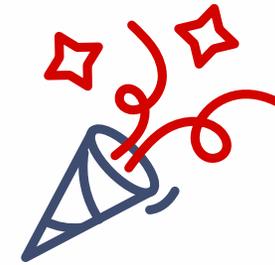
### Trigger prototypes

All templates / TMC Template Module IIS Pool Me... Discovery list / Work Process Pool Win New Relea... Item prototypes 1 Trigger prototypes 2 Graph prototypes 1 Host prototypes

<input type="checkbox"/>	Severity	Name ▲	Operational data	Expression
<input type="checkbox"/>	Information	RecyclePool_Memory_Usage		Problem: <b>last</b> (/TMC Template Module IIS Pool Memory Usage win 2008 and above/system.run[%windir%\system32\inetsrv\appcmd list wp && echo ! && powershell -c "Get-Process -name \"w3wp!\" && echo ! && echo {#NAME_POOL}])>=\${LIMIT_MEMORY_RECYCLE} Recovery: <b>last</b> (/TMC Template Module IIS Pool Memory Usage win 2008 and above/system.run[%windir%\system32\inetsrv\appcmd list wp && echo ! && powershell -c "Get-Process -name \"w3wp!\" && echo ! && echo {#NAME_POOL}])<=\${LIMIT_MEMORY_RECYCLE}
<input type="checkbox"/>	Information	RestartPool_Memory_Usage		Problem: <b>last</b> (/TMC Template Module IIS Pool Memory Usage win 2008 and above/system.run[%windir%\system32\inetsrv\appcmd list wp && echo ! && powershell -c "Get-Process -name \"w3wp!\" && echo ! && echo {#NAME_POOL}])>=\${LIMIT_MEMORY_RESTART} Recovery: <b>last</b> (/TMC Template Module IIS Pool Memory Usage win 2008 and above/system.run[%windir%\system32\inetsrv\appcmd list wp && echo ! && powershell -c "Get-Process -name \"w3wp!\" && echo ! && echo {#NAME_POOL}])<=\${LIMIT_MEMORY_RESTART}

# Caso práctico - Acción

## Autoremediación IIS-Action



### Action

Action Operations 7

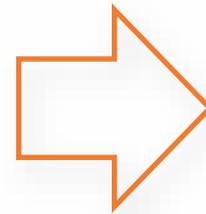
\* Name

Type of calculation  (A or B or C) and D

Conditions	Label	Name
	A	Event name contains <i>url_state</i>
	B	Event name contains <i>Trigger_Memory_Usage</i>
	C	Event name contains <i>pool_state</i>

\* Default operation step duration

Operations	Steps Details	Start in	Durati
1	Run script "Script 9" on current host	Immediately	1m
1-2	Send message to users: iis.mw.p1 (iis.mw.p1 iis.mw.p1), Middleware.tc (Middleware.tc Middleware.tc), NotificacionP1MON (Notificaciones P1 Monitoreo), testjfdt (testjfdt) via all media	Immediately	1m
2	Run script "Script 9" on current host	00:01:00	1m
3	Run script "Script 9" on current host	00:02:00	5m
4	Run script "Script 9" on current host	00:07:00	1m
8	Send message to users: testjfdt (testjfdt) via all media	00:11:00	2m
9	Send message to users: Middleware.tc (Middleware.tc Middleware.tc), Monitoreo_Sonda (Monitoreo_Sonda Monitoreo_Sonda), NotificacionP1MON (Notificaciones P1 Monitoreo), testjfdt (testjfdt) via all media	00:13:00	2m



**Pasamos de tener:**

**3 INC críticos** diarios por consumo de memoria de los app\_pool.

**A:**

**0 INC críticos** diarios por consumo de memoria de los app\_pool.

# Tips para autoremediar:



- Identifique la necesidad a resolver.



- Haga un análisis 80/20 de la situación.



- Realice un “journey” al proceso que desea mejorar, defina KPIs.



- Identifique e implemente los monitores, triggers, actions que requiera.



- Asegure esquema de reintentos.



- Tabule los eventos de automatización y autoremediación



- Valide captura de valor vs KPI.



- Realice ajustes necesarios.

# ¿Qué tenemos en 7.0?

# ZBXNEXT-297

## Remote command execution by active agents

```
{
  "response": "success",
  "config_revision": 2,
  "data": [
    {
      "key": "system.uptime",
      "itemid": 1234,
      "delay": "10s",
      "lastlogsize": 0,
      "mtime": 0
    },
    {
      "key": "agent.version",
      "itemid": 5678,
      "delay": "10m",
      "lastlogsize": 0,
      "mtime": 0,
      "timeout": "30s"
    }
  ],
  "commands": [
    {
      "command": "df -h --output=source,size / | awk 'NR>1 {print $2}'",
      "id": 1324,
      "wait": 1
    }
  ]
}
```

# ZBXNEXT-1096

Configurable Timeout por item  
Hasta 10 minutos

Timeouts ▾

Timeouts for item types

* Zabbix agent	<input type="text" value="3s"/>
* Simple check	<input type="text" value="3s"/>
* SNMP agent	<input type="text" value="3s"/>
* External check	<input type="text" value="3s"/>
* Database monitor	<input type="text" value="3s"/>
* HTTP agent	<input type="text" value="3s"/>
* SSH agent	<input type="text" value="3s"/>
* TELNET agent	<input type="text" value="3s"/>
* Script	<input type="text" value="3s"/>

Network timeouts for UI

* Communication	<input type="text" value="3s"/>
* Connection	<input type="text" value="3s"/>
* Media type test	<input type="text" value="65s"/>
* Script execution	<input type="text" value="60s"/>
* Item test	<input type="text" value="60s"/>
* Scheduled report test	<input type="text" value="60s"/>

\*\*\*E

\*\*\*This document is classified as PUBLIC by TELEFONICA.

# ZBXNEXT-6974

## Trigger top 100, extend filtering

Top 100 triggers

?

Zoom out Last 3 months Filter

Host groups   Problem tags

Hosts

Problem

Severity  Not classified  Warning  High  
 Information  Average  Disaster

Host	Trigger	Severity	Number of problems
<a href="#">Zabbix server 7.0</a>	<a href="#">Linux: Zabbix server 7.0 has been restarted</a>	Warning	2
<a href="#">Zabbix server 7.0</a>	<a href="#">Linux: Operating system description has changed</a>	Information	2
<a href="#">Zabbix server 6.0</a>	<a href="#">Linux: Zabbix agent is not available</a>	Average	1
<a href="#">Zabbix server 7.0</a>	<a href="#">Linux: Number of installed packages has been changed</a>	Warning	1
<a href="#">Zabbix server 7.0</a>	<a href="#">Zabbix server: Version has changed</a>	Information	1

# ZBXNEXT-8638

## New trigger functions jsonpath, xpath

`jsonpath(value,path,<default>)`

Return the JSONPath result.

Supported value types: *String, Text, Log*.

Parameters:

- **value** - the value to check;
- **path** - the path (must be quoted);
- **default** - the optional fallback value if the JSONPath query returns no data.

Example:

```
jsonpath(last(/host/proc.get[zabbix_agentd,,,summary]),"$..size")
```



# ZBXNEXT-9150

## Browser monitoring

The screenshot shows the Zabbix LOG interface. At the top, there are tabs for SYSTEM, EVENT, NETWORK, and LOG. The LOG tab is active. Below the tabs, there are filters for Start Time (2015-10-23 00:00:00), End Time (2015-10-24 00:00:00), and Type (All). A search bar is also present. The main area displays a table of log entries with columns for ID, Time, Event, Play, and Details. The table shows various system events such as 'Save <Storage Setup> config!', 'Modify User<888888>', 'User logged in.<888888>', and 'Shutdown [15-10-23 07:23:40]'. At the bottom, there are navigation buttons like PgUp, PgDn, Go To, Page(s), Backup, and Clear.

ID	Time	Event	Play	Details
29	2015-10-23 07:16:48	Save <Storage Setup> config!	--	
30	2015-10-23 07:16:48	Modify User<888888>	--	
31	2015-10-23 07:16:48	Modify User<admin>	--	
32	2015-10-23 07:16:48	Modify User<default>	--	
33	2015-10-23 07:16:48	HDD Totals<1>, Current Working HI	--	
34	2015-10-23 07:23:08	User logged in.<888888>	--	
35	2015-10-23 07:24:08	Format HDD<2>	--	
36	2015-10-23 07:25:27	Shutdown [15-10-23 07:23:40]	--	
37	2015-10-23 07:25:27	Reboot with Flag [0x00]	--	
38	2015-10-23 07:25:27	Modify User<888888>	--	
39	2015-10-23 07:25:27	Modify User<admin>	--	
40	2015-10-23 07:25:27	Modify User<default>	--	
41	2015-10-23 07:25:27	HDD Totals<1>, Current Working HI	--	
42	2015-10-23 07:26:27	User logged in.<888888>	--	

Item Tags Preprocessing

\* Name

Type

\* Key

Type of information

Parameters

Name	Value	Action
<input type="text"/>	<input type="text"/>	<a href="#">Remove</a>

[Add](#)

\* Script

Units

\* Update interval

Custom intervals

Type	Interval	Period	Action
<input checked="" type="checkbox"/> Flexible <input type="checkbox"/> Scheduling	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>	<a href="#">Remove</a>

[Add](#)

\* Timeout  Global  Override  [Timeouts](#)

\* History

\* Trends



ZABBIX '24  
CONFERENCE  
LATIN AMERICA

# ¡Gracias!



[www.Imgunet.com](http://www.Imgunet.com)



Síguenos en **LinkedIn**



Síguenos en **YouTube**



Síguenos en **Instagram**

# Insert title

First level

Second level

Third level

# Insert title

First level

Second level

Third level



# Insert title

First level

Second level

Third level

Thank you!

