Monitoramento de equipamentos em infraestrutura de rede com Zabbix

Rafael Barasuol Rohden

QUEM SOU?

- Formação
  - Informática - Sistemas de informação (UNIJUI-2010)
  - Msc. Ciência da Computação (UFSM-2015)

- Experiências Antigas
  - 6 anos: desenvolverdor PHP, MYSQL, HTML, CSS, JavaScript.

- Atualmente
  - 3 anos: Professor Ciência da Computação (UNICRUZ)
  - 3 anos: Analista de Informática (CERILUZ)

Agenda

- Zabbix
  - Funcionalidades e Diferentes abordagens
  - Arquitetura básica
  - Conceitos Zabbix
- Monitoramento
  - Agentes
  - Hosts e itens
  - SNMP e MIB
- Caso de Estudo
  - CERILUZ

Porque monitorar minha rede?

- É difícil de gerenciar um ambiente heterogênio
- O custo do tempo de inatividade é alto
- Minimizar o impacto nos negócios
- Saber se seu serviço está acessível

Funcionalidades Zabbix

✓ Coleta de Dados

Usando vários métodos, incluindo SNMP, agentes nativos, IPMI e outros

✓ Detecção e alerta de problemas

Os dados coletados podem ser comparados aos limites e alertas enviados usando diferentes canais, como email ou SMS

✓ Histórico

Depois de coletar os dados, não faz sentido jogá-los fora, por isso, muitas vezes, queremos armazená-los para análise posterior

✓ Visualização

Os seres humanos são melhores em distinguir dados visualizados, dando importancia as informações dependendo de suas necessidades

SNMP?

- Simple Network Management Protocol (Protocolo Simples de Gerência de Rede)

- Dispositivos que normalmente suportam SNMP

  – roteadores, computadores, servidores, estações de trabalho, impressoras, racks modernos, sensores de temperatura e etc.

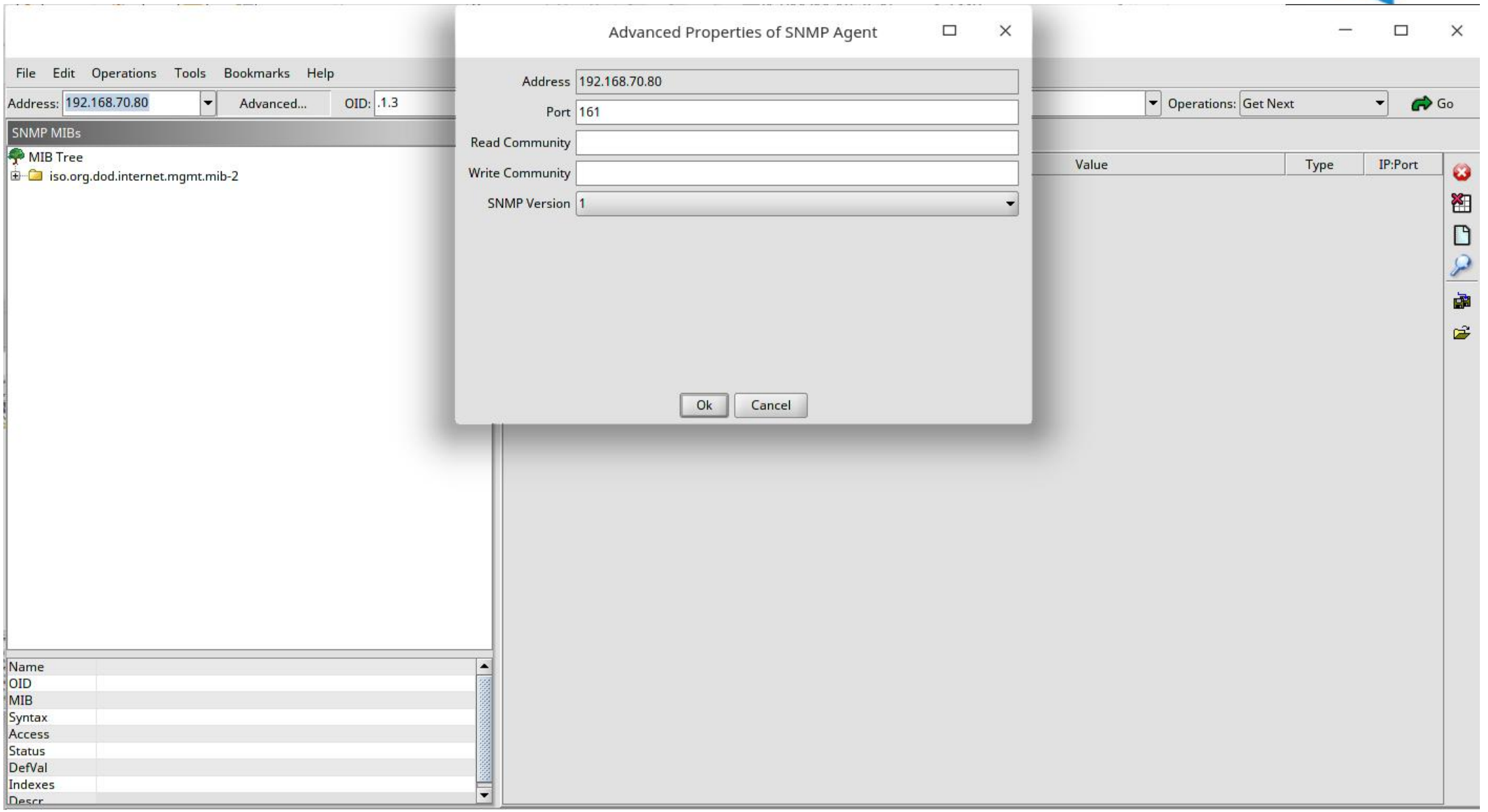
SNMP

- Uma rede SNMP é caracterizada por três componentes fundamentais:
  - Dispositivos gerenciados
  - Agentes
  - Sistemas de Gestão de Redes
    - (NMS - Network Management System)

MIB

- Management Information Base
  - A descrição de cada elemento de rede
  - Variáveis de estado
  - Estão descritas e armazenadas em bancos de dados virtuais chamados MIBs
  - Em uma estrutura hierárquica, identificadores de objetos (OIDs) permitem a distinção de cada variável que pode ser acessada para escrita ou leitura via SNMP.

MIB Browser


Advanced Properties of SNMP Agent
Address 192.168.70.80
Port 161
Read Community
Write Community
SNMP Version 1
Ok
Cancel
File Edit Operations Tools Bookmarks Help
Address: 192.168.70.80
Advanced...
OID: .1.3
Operations: Get Next
Go
SNMP MIBs
MIB Tree
iso.org.dod.internet.mgmt.mib-2
Value
Type
IP:Port
Name
OID
MIB
Syntax
Access
Status
DefVal
Indexes
Descr

MIB Browser

iReasoning MIB Browser

Operations: Get Next

Go

Result Table

Name/OID	Value	Type	IP:Port
sysDescr.0	24-port 10/100/1000 Gigabit Switch	OctetString	192.168.24...
sysObjectID.0	.1.3.6.1.4.1.674.10895.3028	OID	192.168.24...
sysUpTime.0	3105 hours 14 minutes 58 seconds (1117889800)	TimeTicks	192.168.24...
sysContact.0		OctetString	192.168.24...
sysName.0	SW-A2	OctetString	192.168.24...
sysLocation.0	Datacenter A	OctetString	192.168.24...
sysServices.0	2	Integer	192.168.24...
.1.3.6.1.2.1.1.8.0	0 millisecond (0)	TimeTicks	192.168.24...
.1.3.6.1.2.1.1.9.1.2.1	.1.3.6.1.4.1.89.73	OID	192.168.24...
.1.3.6.1.2.1.1.9.1.3.1	RS capabilities	OctetString	192.168.24...
.1.3.6.1.2.1.1.9.1.4.1	0 millisecond (0)	TimeTicks	192.168.24...

MIB Browser

iReasoning MIB Browser

Operations: Get Next

Result Table

Name/OID	Value	Type	IP:Port
ifSpeed.5	1000000000	Gauge	192.168.24...
ifSpeed.6	10000000	Gauge	192.168.24...
ifSpeed.7	1000000000	Gauge	192.168.24...
ifSpeed.8	1000000000	Gauge	192.168.24...
ifSpeed.9	1000000000	Gauge	192.168.24...
ifSpeed.10	1000000000	Gauge	192.168.24...
ifSpeed.11	100000000	Gauge	192.168.24...
ifSpeed.12	100000000	Gauge	192.168.24...
ifSpeed.13	1000000000	Gauge	192.168.24...
ifSpeed.14	1000000000	Gauge	192.168.24...
ifSpeed.15	1000000000	Gauge	192.168.24...
ifSpeed.16	1000000000	Gauge	192.168.24...
ifSpeed.17	1000000000	Gauge	192.168.24...
ifSpeed.18	1000000000	Gauge	192.168.24...
ifSpeed.19	100000000	Gauge	192.168.24...
ifSpeed.20	1000000000	Gauge	192.168.24...
ifSpeed.21	1000000000	Gauge	192.168.24...
ifSpeed.22	1000000000	Gauge	192.168.24...
ifSpeed.23	1000000000	Gauge	192.168.24...
ifSpeed.24	1000000000	Gauge	192.168.24...
ifSpeed.1000	0	Gauge	192.168.24...
ifSpeed.1001	0	Gauge	192.168.24...
ifSpeed.1002	0	Gauge	192.168.24...
ifSpeed.1003	0	Gauge	192.168.24...
ifSpeed.1004	0	Gauge	192.168.24...
ifSpeed.1005	0	Gauge	192.168.24...
ifSpeed.1006	0	Gauge	192.168.24...
ifSpeed.1007	0	Gauge	192.168.24...
ifSpeed.100000	0	Gauge	192.168.24...
ifSpeed.100001	0	Gauge	192.168.24...
ifSpeed.100008	0	Gauge	192.168.24...
ifSpeed.100009	0	Gauge	192.168.24...
ifSpeed.100016	0	Gauge	192.168.24...
ifSpeed.100019	0	Gauge	192.168.24...
ifSpeed.100029	0	Gauge	192.168.24...
ifSpeed.100049	0	Gauge	192.168.24...
ifSpeed.100089	0	Gauge	192.168.24...
ifSpeed.100099	0	Gauge	192.168.24...
ifSpeed.100110	0	Gauge	192.168.24...
ifSpeed.100199	0	Gauge	192.168.24...
ifSpeed.100298	0	Gauge	192.168.24...
ifSpeed.100510	0	Gauge	192.168.24...
ifSpeed.100554	0	Gauge	192.168.24...
ifPhysAddress.1	A4-BA-DB-89-A1-17	OctetString	192.168.24...
ifPhysAddress.2	A4-BA-DB-89-A1-18	OctetString	192.168.24...
ifPhysAddress.3	A4-BA-DB-89-A1-19	OctetString	192.168.24...

MIB Browser

iReasoning MIB Browser

Operations: Get Next

Result Table

Name/OID	Value	Type	IP:Port
ifOperStatus.18	up (1)	Integer	192.168.24...
ifOperStatus.19	up (1)	Integer	192.168.24...
ifOperStatus.20	down (2)	Integer	192.168.24...
ifOperStatus.21	up (1)	Integer	192.168.24...
ifOperStatus.22	up (1)	Integer	192.168.24...
ifOperStatus.23	up (1)	Integer	192.168.24...
ifOperStatus.24	up (1)	Integer	192.168.24...
ifOperStatus.1000	notPresent (6)	Integer	192.168.24...
ifOperStatus.1001	notPresent (6)	Integer	192.168.24...
ifOperStatus.1002	notPresent (6)	Integer	192.168.24...
ifOperStatus.1003	notPresent (6)	Integer	192.168.24...
ifOperStatus.1004	notPresent (6)	Integer	192.168.24...
ifOperStatus.1005	notPresent (6)	Integer	192.168.24...
ifOperStatus.1006	notPresent (6)	Integer	192.168.24...
ifOperStatus.1007	notPresent (6)	Integer	192.168.24...
ifOperStatus.100000	up (1)	Integer	192.168.24...
ifOperStatus.100001	up (1)	Integer	192.168.24...
ifOperStatus.100008	up (1)	Integer	192.168.24...
ifOperStatus.100009	up (1)	Integer	192.168.24...
ifOperStatus.100016	down (2)	Integer	192.168.24...
ifOperStatus.100019	up (1)	Integer	192.168.24...
ifOperStatus.100029	up (1)	Integer	192.168.24...
ifOperStatus.100049	up (1)	Integer	192.168.24...
ifOperStatus.100089	up (1)	Integer	192.168.24...
ifOperStatus.100099	up (1)	Integer	192.168.24...
ifOperStatus.100110	up (1)	Integer	192.168.24...
ifOperStatus.100199	up (1)	Integer	192.168.24...
ifOperStatus.100298	up (1)	Integer	192.168.24...
ifOperStatus.100510	up (1)	Integer	192.168.24...
ifOperStatus.100554	down (2)	Integer	192.168.24...
ifLastChange.1	812 hours 55 minutes 48 seconds (292654884)	TimeTicks	192.168.24...
ifLastChange.2	21 seconds (2146)	TimeTicks	192.168.24...
ifLastChange.3	812 hours 55 minutes 54 seconds (292655438)	TimeTicks	192.168.24...
ifLastChange.4	812 hours 56 minutes 7 seconds (292656716)	TimeTicks	192.168.24...
ifLastChange.5	984 hours 52 minutes 33 seconds (354555308)	TimeTicks	192.168.24...
ifLastChange.6	25 seconds (2548)	TimeTicks	192.168.24...
ifLastChange.7	21 seconds (2172)	TimeTicks	192.168.24...
ifLastChange.8	25 seconds (2554)	TimeTicks	192.168.24...
ifLastChange.9	314 hours 25 minutes 6 seconds (113190694)	TimeTicks	192.168.24...
ifLastChange.10	1056 hours 21 minutes 49 seconds (380290918)	TimeTicks	192.168.24...
ifLastChange.11	714 hours 50 minutes 17 seconds (257341728)	TimeTicks	192.168.24...
ifLastChange.12	28 seconds (2882)	TimeTicks	192.168.24...
ifLastChange.13	713 hours 9 minutes 11 seconds (256735132)	TimeTicks	192.168.24...
ifLastChange.14	576 hours 11 minutes (207426070)	TimeTicks	192.168.24...
ifLastChange.15	22 seconds (2222)	TimeTicks	192.168.24...
ifLastChange.16	613 hours 41 minutes 31 seconds (220929170)	TimeTicks	192.168.24...
ifLastChange.17	22 seconds (2232)	TimeTicks	192.168.24...
ifLastChange.18	504 hours 51 minutes 35 seconds (181749586)	TimeTicks	192.168.24...

Diferentes Abordagens

Monitoramento sem agente

- ✓ Ping ICMP
- ✓ HTTP, SSH, IMAP, SMTP, outros serviços
- ✓ Comandos remotos usando Telnet e SSH

Monitoramento com agente

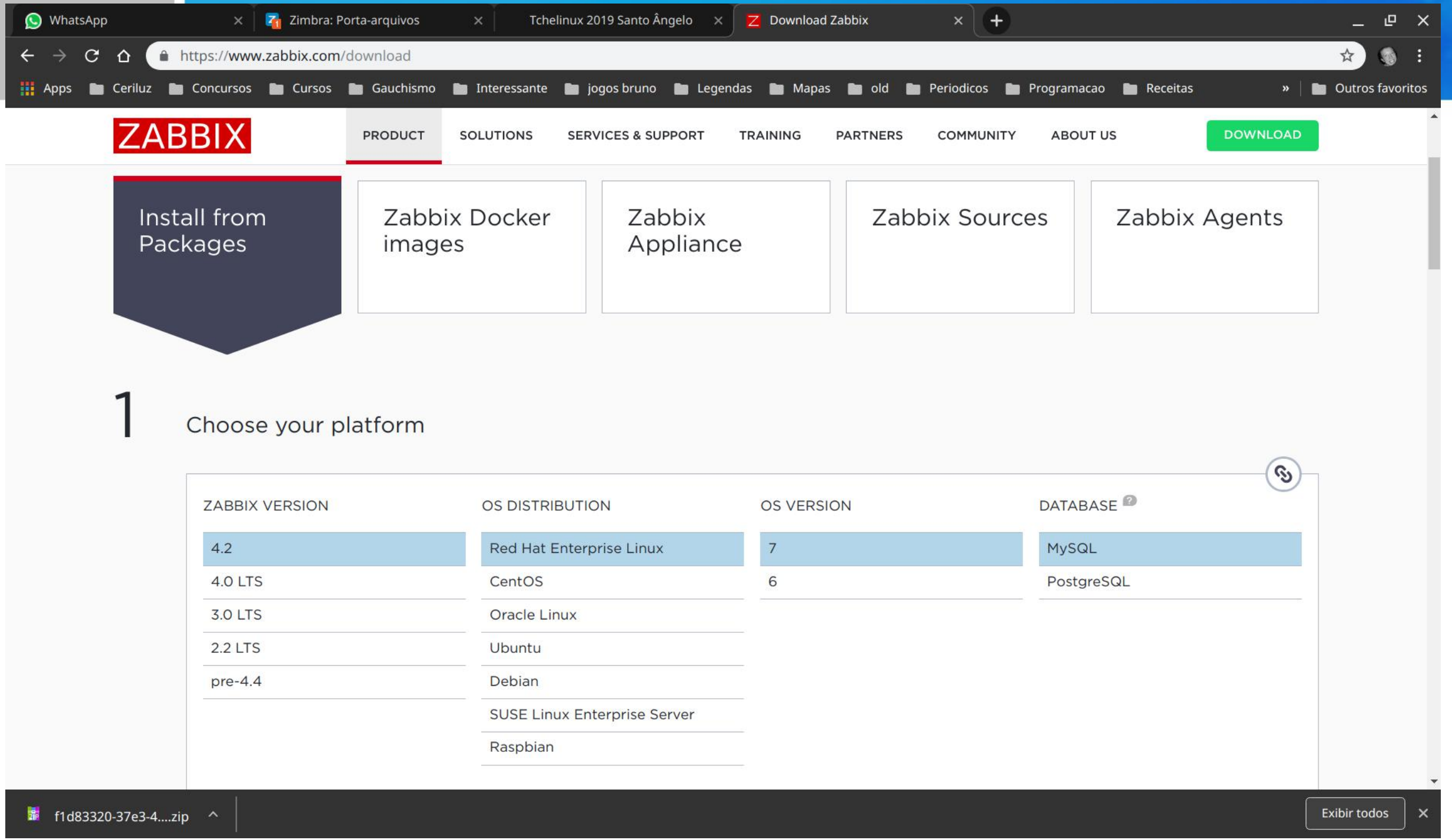
- ✓ Agentes passivos
  - ✓ SNMP, Agente Zabbix, IPMI
- ✓ Agentes ativos
  - ✓ Armadilhas SNMP, Agente Zabbix

Monitoramento Centralizado

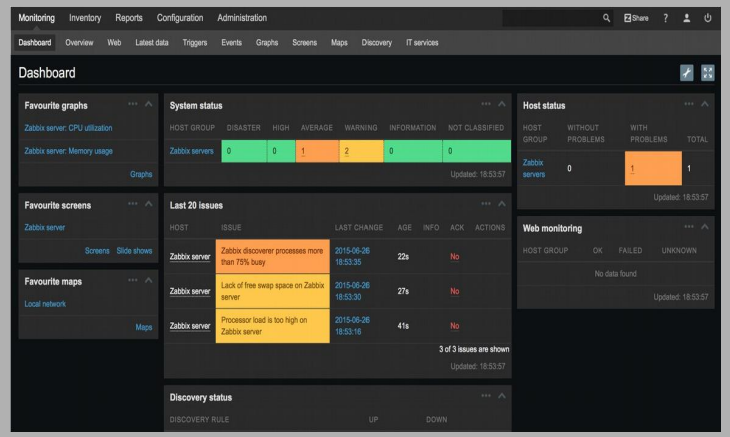
- ✓ Toda a configuração e gerenciamento são feitos em um servidor Zabbix central

Monitoramento distribuído

- ✓ Reduzir a carga de rede
- ✓ Link para sobreviver ao tempo de inatividade


WhatsApp
Zimbra: Porta-arquivos
Tchelinux 2019 Santo Ângelo
Download Zabbix
https://www.zabbix.com/download
Apps
Ceriluz
Concursos
Cursos
Gauchismo
Interessante
jogos bruno
Legendas
Mapas
old
Periodicos
Programacao
Receitas
Outros favoritos
ZABBIX
PRODUCT
SOLUTIONS
SERVICES & SUPPORT
TRAINING
PARTNERS
COMMUNITY
ABOUT US
DOWNLOAD
Install from Packages
Zabbix Docker images
Zabbix Appliance
Zabbix Sources
Zabbix Agents
1
Choose your platform
ZABBIX VERSION
4.2
4.0 LTS
3.0 LTS
2.2 LTS
pre-4.4
OS DISTRIBUTION
Red Hat Enterprise Linux
CentOS
Oracle Linux
Ubuntu
Debian
SUSE Linux Enterprise Server
Raspbian
OS VERSION
7
6
DATABASE
MySQL
PostgreSQL
f1d83320-37e3-4....zip
Exibir todos

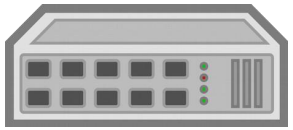
Arquitetura Básica I



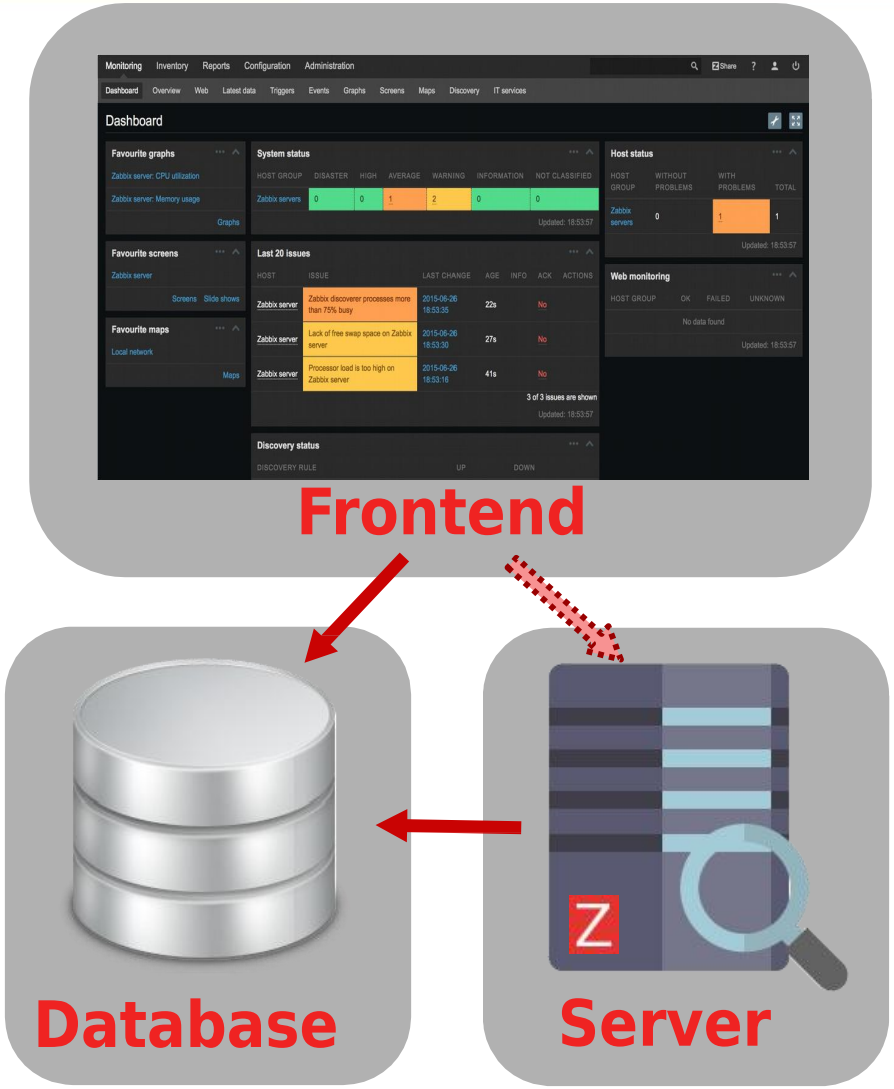
Frontend

Database

Server



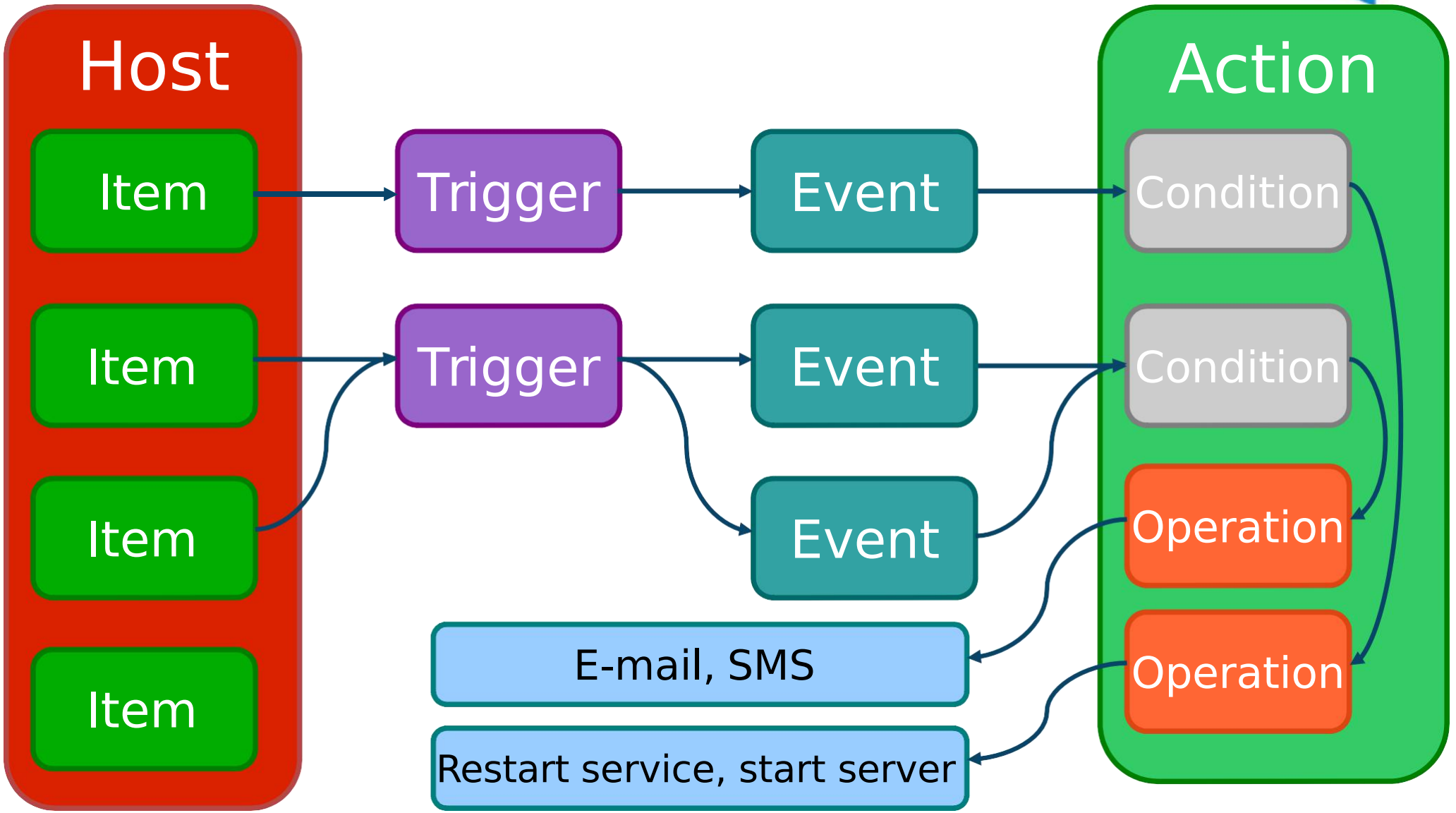
Arquitetura Básica II



Definições

Componentes	Definição
Host	Qualquer dispositivo conectado à rede com IP ou nome no DNS
Host Group	Agrupamento lógico de hosts em grupo
Item	Fonte de informação / métrica
Trigger	Expressão lógica que representa a condição do problema
Template	Um conjunto de entidades (itens, gatilhos, etc.) prontos para serem aplicados a um ou vários hosts
Application	Agrupamento de itens em um grupo lógico
Event	Alteração do estado do elemento
Action	Um conjunto flexível de condições. Conjunto de operações executado automaticamente
Operation	Tipos diferentes: notificação, comando remoto, adicionar / remover host, vinculação de modelo

Funcionamento



HOST

Hosts

Host | Templates | IPMI | Macros | Host inventory

Host name: New host

Visible name:

Groups

In groups: Linux servers

Other groups: Database servers, Discovered hosts, Hypervisors, Network devices, Templates, UPS devices, Virtual machines, Web servers, Windows servers, Zabbix servers

New group:

Agent interfaces

IP address	DNS name	Connect to	Port	Default
127.0.0.1		IP DNS	10050	Remove

Add

SNMP interfaces: Add

JMX interfaces: Add

IPMI interfaces: Add

Description:

Monitored by proxy: (no proxy)

Enabled: ☑

Add | Cancel

ITEM

Items

All hosts / New host Enabled ZBX SNMP JMX IPMI Applications Items 1 Triggers Graphs

Name	CPU Load
Type	Zabbix agent
Key	system.cpu.load Select
Host interface	192.168.3.31 : 32050
Type of information	Numeric (float)
Units	
Use custom multiplier	☐ 1
Update interval (in sec)	30
Flexible intervals	Interval Period Action No flexible intervals defined.
New flexible interval	Interval (in sec) 50 Period 1-7,00:00-24:00 Add
History storage period (in days)	7
Trend storage period (in days)	365
Store value	As is
Show value	As is show value mappings
New application	
Applications	-None-
Populates host inventory field	-None-
Description	
Enabled	☑

Add Cancel

ITEM

All hosts / SW-A2 Enabled ZBX SNMP JMX IPMI Applications 11 Items 323 Triggers 42 Graphs 33 Discovery rules 2 Web scenarios

Parent items	DELL 2824
Name	State of the FAN 1
Type	SNMPv2 agent
Key	stateFan1
Host interface	192.168.249.2 : 161
SNMP OID	.1.3.6.1.4.1.89.53.15.1.4.1
SNMP community	{$SNMP_COMMUNITY}
Port	
Type of information	Numeric (unsigned)
Data type	Decimal
Units	
Use custom multiplier	1
Update interval (in sec)	30

Custom intervals

Type	Interval	Period	Action
Flexible / Scheduling	50	1-7,00:00-24:00	Remove

Add

History storage period (in days)	90
Trend storage period (in days)	365
Store value	As is
Show value	FAN Map

show value mappings

Trigger

Triggers

All hosts / New host Enabled ZBX SNMP JMX IPMI Applications Items 2 Triggers 1 Graphs

Trigger Dependencies

Name: CPU load too high on 'New host' for 3 minutes

Expression: {New host:system.cpu.load.avg(180)}>5 Add

Expression constructor

Multiple PROBLEM events generation: ☐

Description:

URL:

Severity: Not classified | Information | Warning | Average | High

Enabled: ☑

Add Cancel

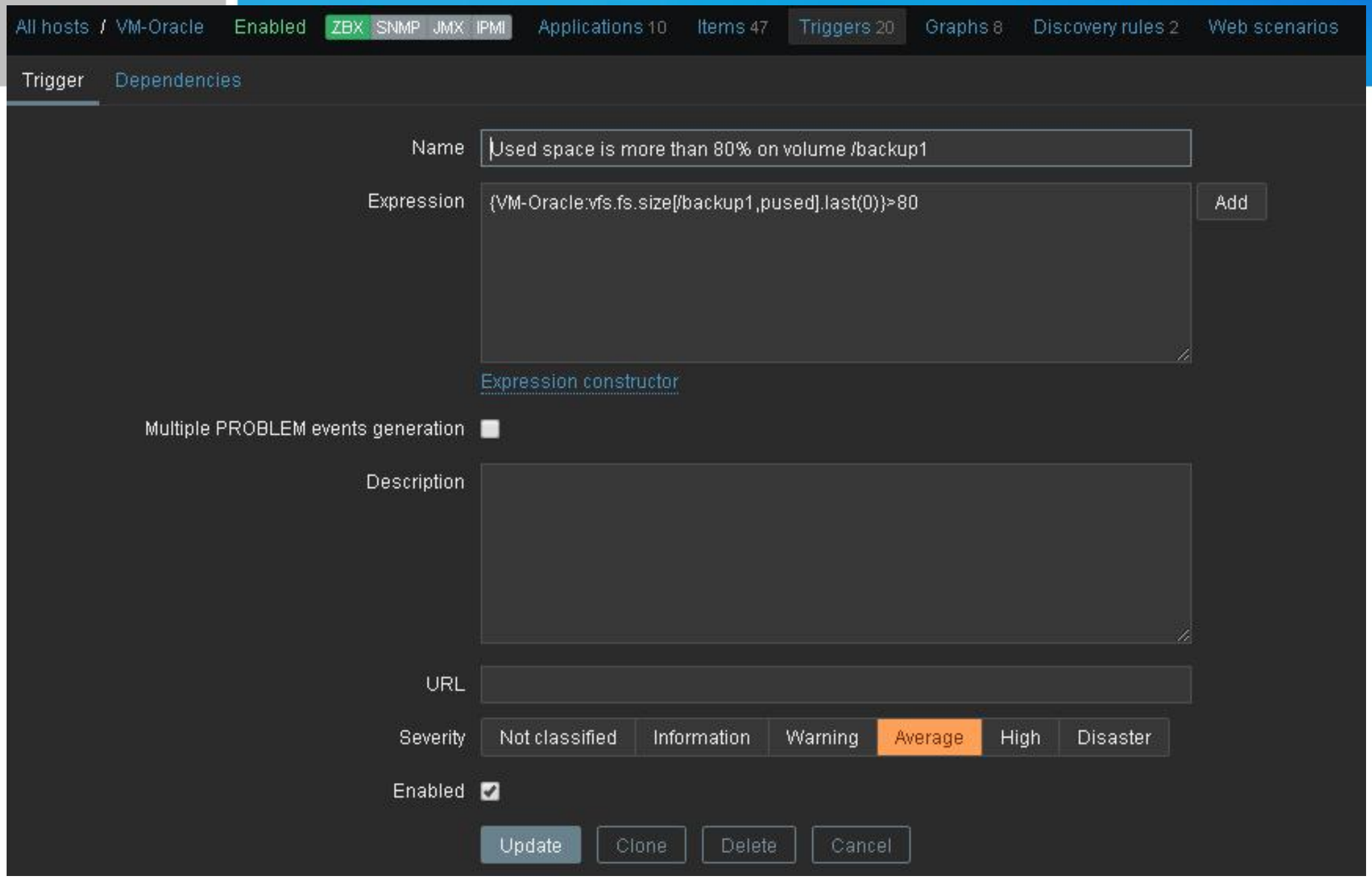
Status of triggers

Group all Host all

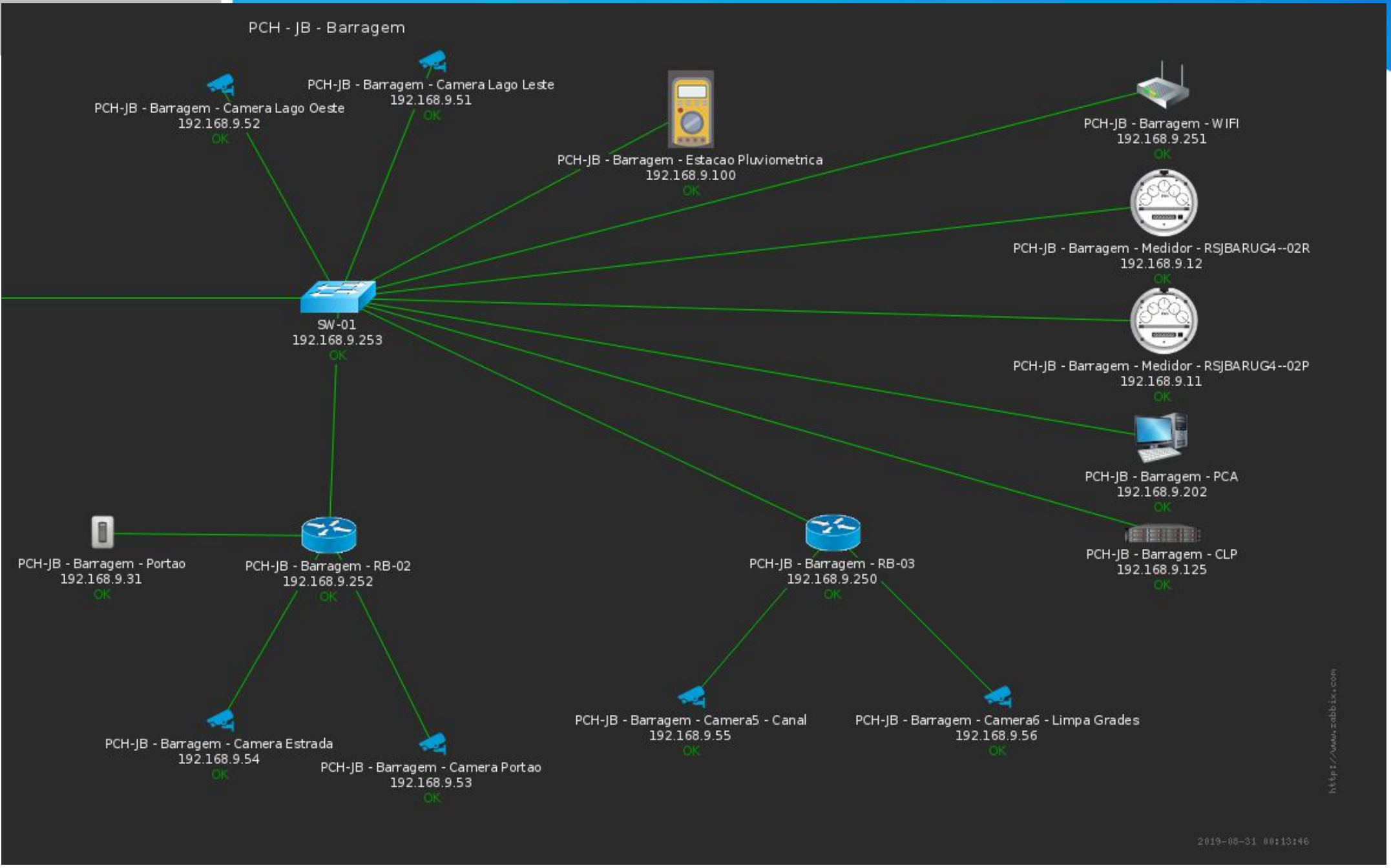
Filter

SEVERITY	STATUS	INFO	LAST CHANGE	AGE	ACK	HOST	NAME	DESCRIPTION
Not classified	OK		2015-08-08 21:08:49	5s	No 1	New host	CPU load too high on 'New host' for 3 minutes	Add

Trigger


All hosts / VM-Oracle
Enabled
ZBX SNMP JMX IPMI
Applications 10
Items 47
Triggers 20
Graphs 8
Discovery rules 2
Web scenarios
Trigger
Dependencies
Name
Used space is more than 80% on volume /backup1
Expression
{VM-Oracle:vfs.fs.size[/backup1,pused].last(0)}>80
Add
Expression constructor
Multiple PROBLEM events generation
Description
URL
Severity
Not classified
Information
Warning
Average
High
Disaster
Enabled
Update
Clone
Delete
Cancel

MAPS


PCH - JB - Barragem
PCH-JB - Barragem - Camera Lago Oeste
192.168.9.52
OK
PCH-JB - Barragem - Camera Lago Leste
192.168.9.51
OK
PCH-JB - Barragem - Estacao Pluviometrica
192.168.9.100
OK
PCH-JB - Barragem - WIFI
192.168.9.251
OK
PCH-JB - Barragem - Medidor - RSJBARUG4--02R
192.168.9.12
OK
SW-01
192.168.9.253
OK
PCH-JB - Barragem - Medidor - RSJBARUG4--02P
192.168.9.11
OK
PCH-JB - Barragem - PCA
192.168.9.202
OK
PCH-JB - Barragem - CLP
192.168.9.125
OK
PCH-JB - Barragem - Portao
192.168.9.31
OK
PCH-JB - Barragem - RB-02
192.168.9.252
OK
PCH-JB - Barragem - RB-03
192.168.9.250
OK
PCH-JB - Barragem - Camera Estrada
192.168.9.54
OK
PCH-JB - Barragem - Camera Portao
192.168.9.53
OK
PCH-JB - Barragem - Camera5 - Canal
192.168.9.55
OK
PCH-JB - Barragem - Camera6 - Limpa Grades
192.168.9.56
OK
http://www.zabbix.com
2019-08-31 00:13:46

Integração Telegram

- Ter uma conta no telegram
- Criar Bot
- Obter o ID do usuário de destino
- Criar Script

Criando BOT

- Procurar **@BotFather**
- Enviar mensagem **/newbot**
- Informar o nome do bot
  - Meu Bot
- Informar o username do bot
  - meu_bot

- O usuário @BotFather irá retornar um token
  - **524847700:AAHY87465Evmrhc8PX6Ow8LxkgT3zPtW6A**

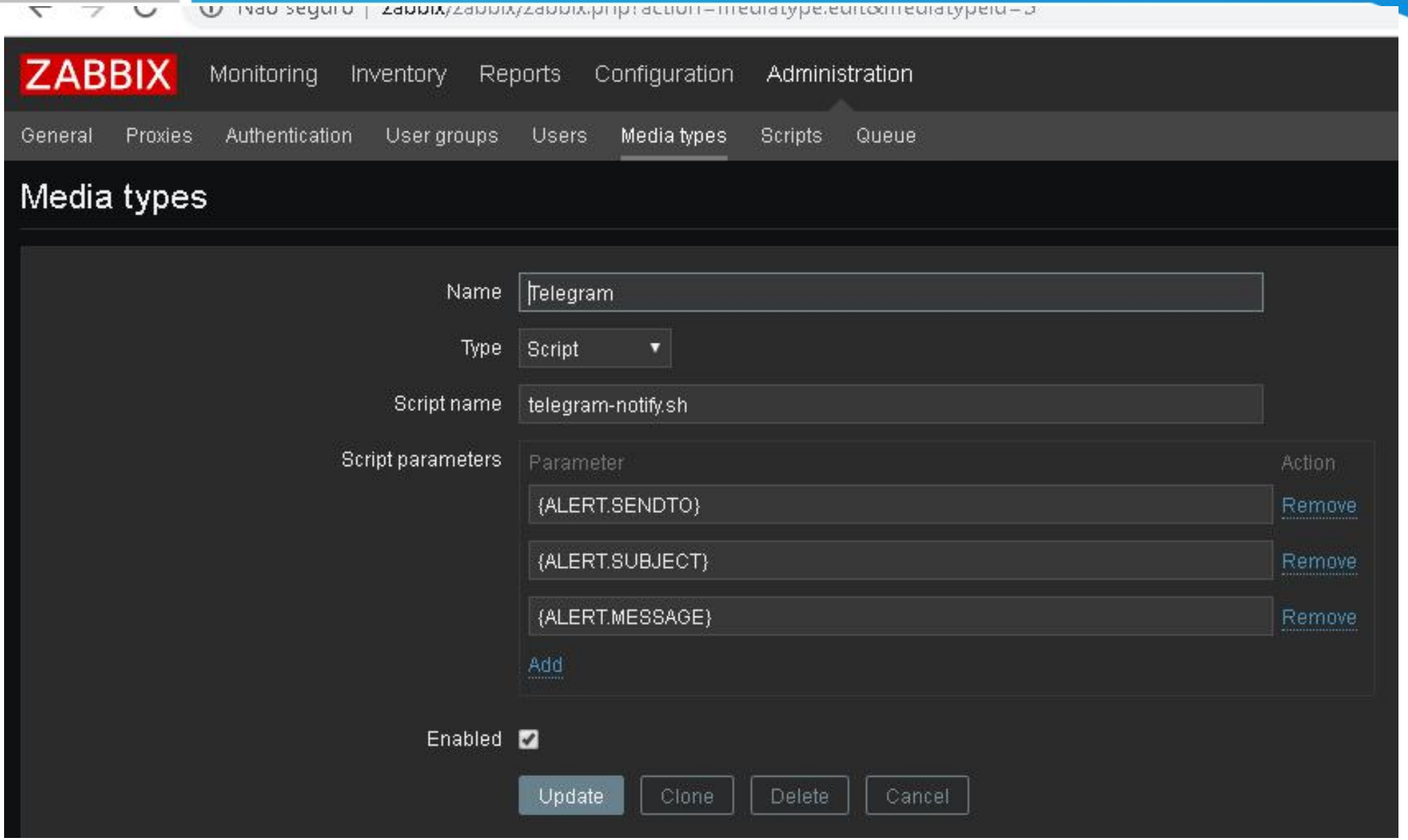
Integração Telegram

- São dois scripts
  - telegram-getUpdates.sh
  - telegram-notify.sh

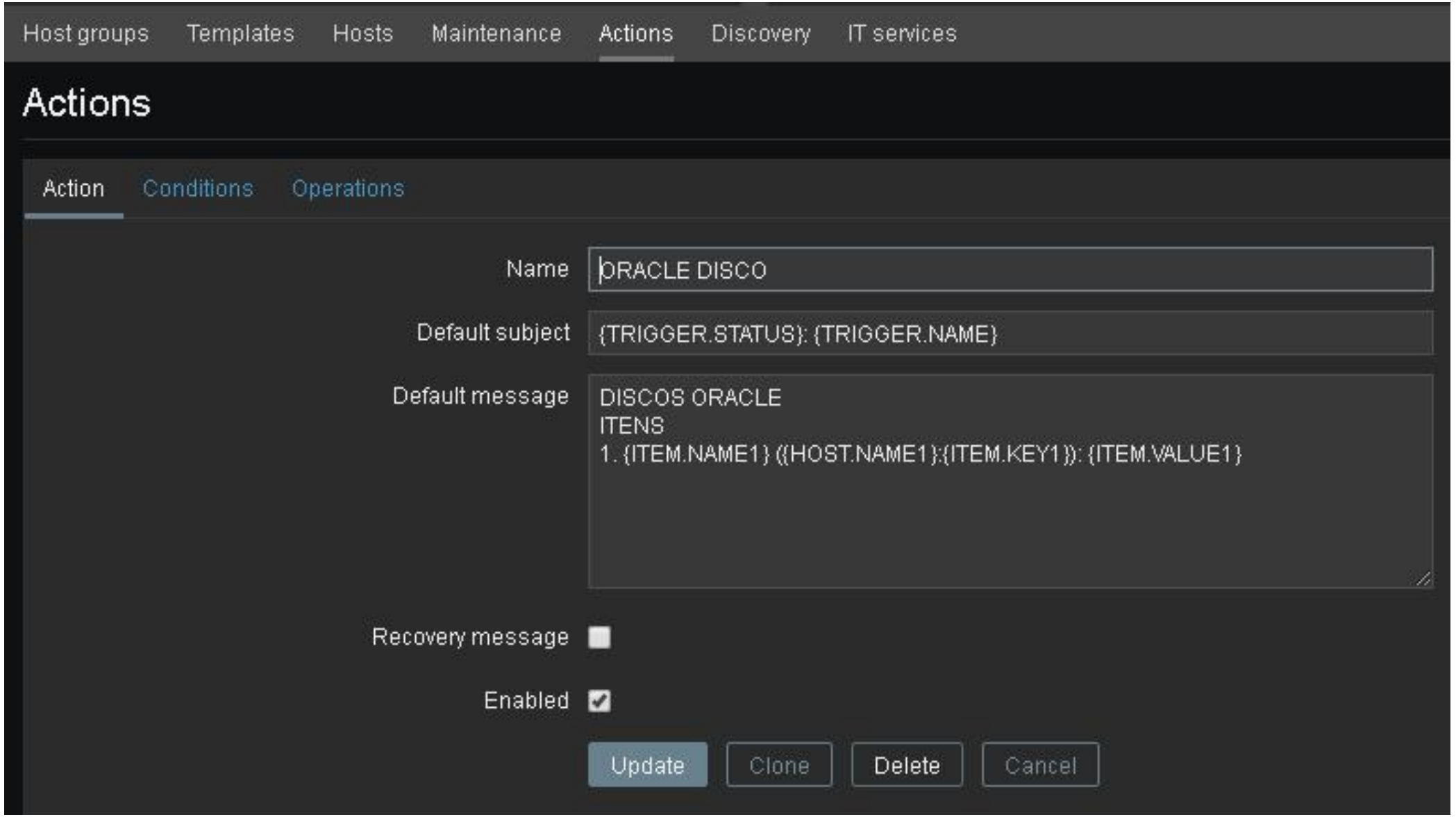
- São colocados no diretório:
  - /usr/lib/zabbix/externalscritps/

- Adicionar token nos scripts

Integração Telegram



Integração Telegram



Integração Telegram

Actions

Action | Conditions | Operations

Type of calculation: Custom expression ▼ | A and B and (C or D or E)

Conditions

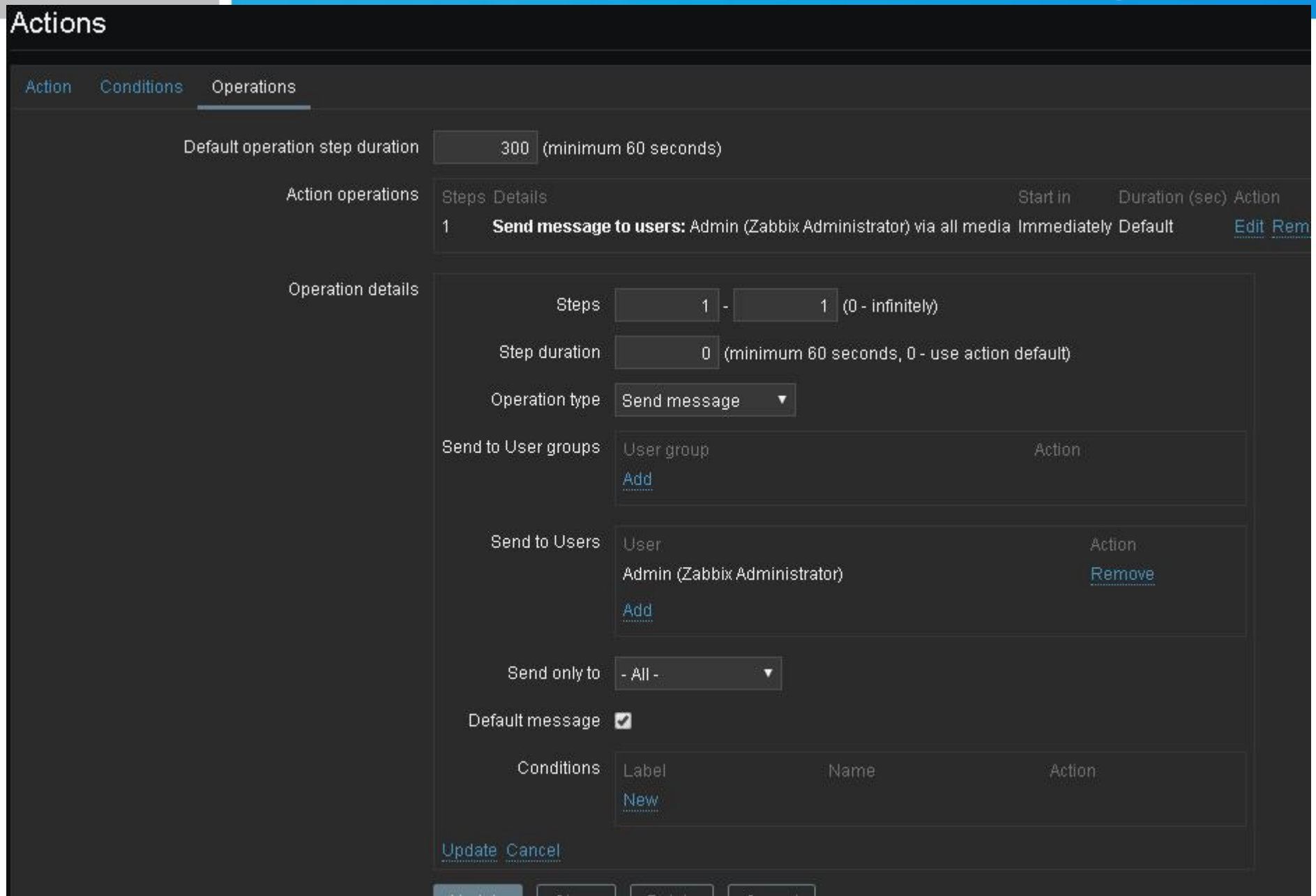
Label	Name	Action
A	Trigger value = *PROBLEM*	Remove
B	Host = *VM-Oracle*	Remove
C	Trigger = *VM-Oracle: Used space is more than 80% on volume /backup1*	Remove
D	Trigger = *VM-Oracle: Used space is more than 80% on volume /backup2*	Remove
E	Trigger = *VM-Oracle: /backup1 perdeu conexão com ISCSI*	Remove

New condition: Trigger name ▼ | like ▼ |

Add

Update | Clone | Delete | Cancel

Integração Telegram



Integração Telegram

General | Proxies | Authentication | User groups | Users | Media types | Scripts | Queue

Users

User | Media | Permissions

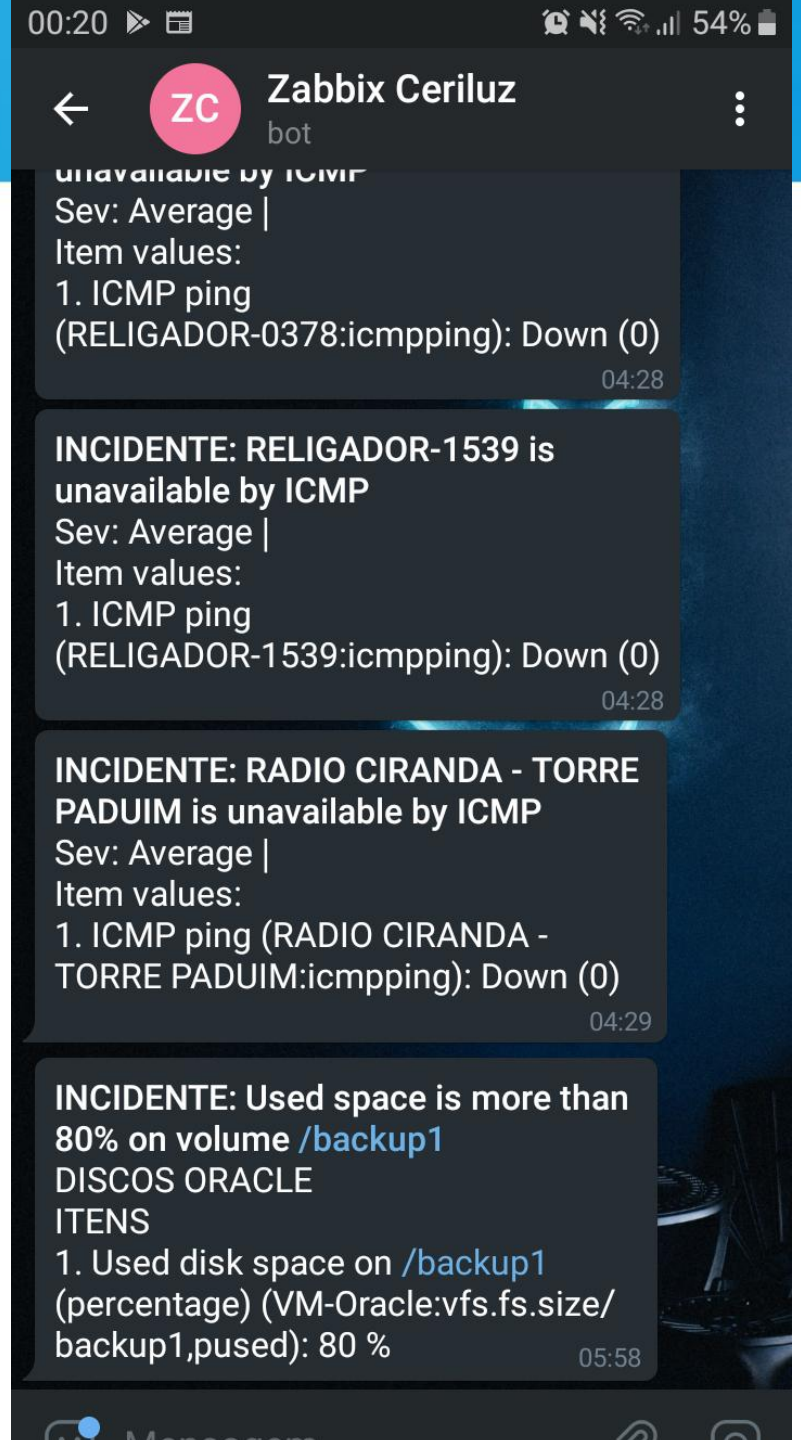
Media

Type	Send to	When active	Use if severity	Status	Action
SMS WebService	55991314017	1-7,00:00-24:00	NIWAHD	Disabled	Edit Remove
SMS WebService	55991579150	1-7,00:00-24:00	NIWAHD	Disabled	Edit Remove
Telegram	481357042	1-7,00:00-24:00	NIWAHD	Enabled	Edit Remove
Telegram	511651343	1-7,00:00-24:00	NIWAHD	Enabled	Edit Remove
Telegram	614944932	1-7,00:00-24:00	NIWAHD	Enabled	Edit Remove
Telegram	616709689	1-7,00:00-24:00	NIWAHD	Enabled	Edit Remove

Add

Update | Delete | Cancel

Integração Telegram



OBRIGADO

PERGUNTAS?

rafaelrohden@gmail.com