ZABBIX

QUEM SOU EU?

ZABBIX

Victor Breda Credidio

- Formado em Ciência da computação;
- Pós-graduado em Segurança da informação;
- LPIC-01/Comptia Linux+
- Zabbix Certified Trainer
- Engenheiro de Suporte Global

/in/victor-bc

ZABBIX

ZABBIX

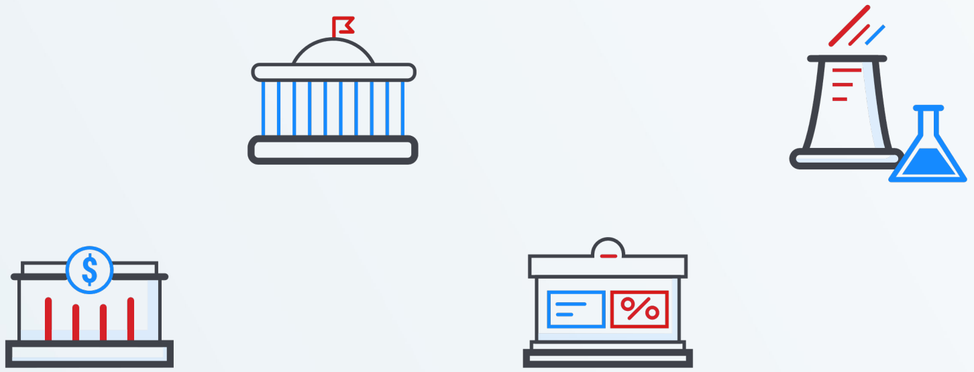
MONITORAMENTO DE ATIVOS EM PROVEDORES UTILIZANDO O ZABBIX COMO SOLUÇÃO

SOBRE O ZABBIX

ZABBIX

O ZABBIX É UMA SOLUÇÃO OPEN SOURCE, GRATUITA, E DE CLASSE EMPRESARIAL, QUE FORNECE MONITORAMENTO EM VÁRIOS NÍVEIS

É UTILIZADO MUNDO A FORA POR EMPRESAS DE VÁRIOS SEGUIMENTOS COMO TELECOMUNICAÇÕES, FINANCEIRO, EDUCACIONAL, VAREJO, E COMPANHIAS DE VÍNCULO HOSPITALAR



O QUE É MONITORAMENTO?

ZABBIX

DEFINIÇÃO DE MONITORAMENTO

“Um contínuo processo de coleta e análise de métricas sobre um programa, projeto, ou negócio, e comparação entre resultados atuais e resultados planejados, de forma a julgar o andamento de sua implementação.”

Fonte: *International Labor Organization*

- **CONTROLE**
- **VISIBILIDADE**
- **ALCANÇAR OBJETIVOS/METAS COM MENOR NÚMERO DE DESVIOS**

POR QUÊ MONITORAR?

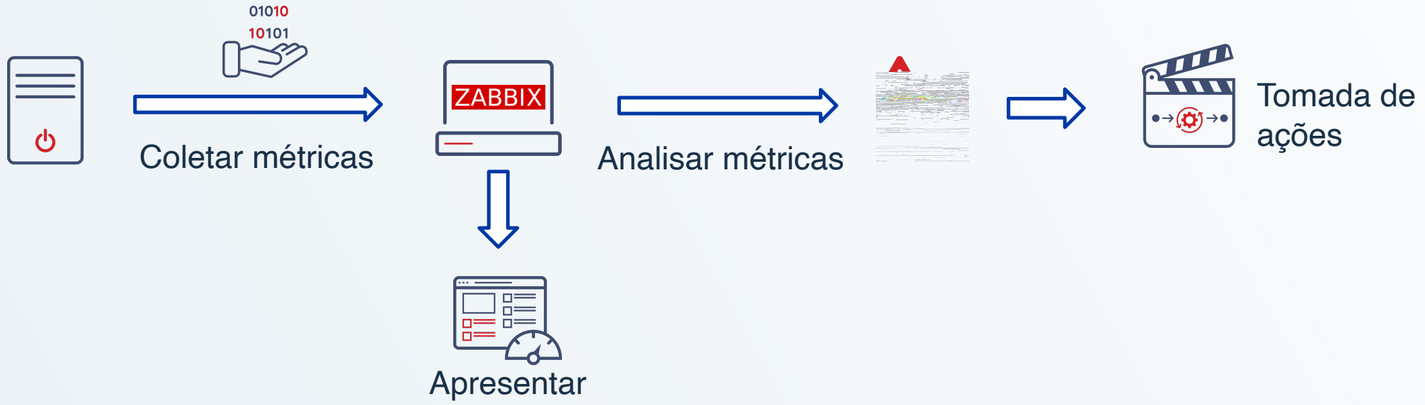
ZABBIX

PERGUNTAS ESSENCIAIS PARA DEFINIR UM SISTEMA DE MONITORAMENTO

- O que será monitorado e quais os indicadores?
- Qual o dado necessário para rastrear o progresso desses indicadores?
- Que tipo de dado precisamos coletar?
- Temos uma baseline apropriada para ser usada como referência?
- Temos uma reserva financeira para implementar as ferramentas necessárias para realizar o monitoramento?
- Temos uma equipe preparada para lidar com essa ferramenta?
- O sistema a ser implementado oferece recursos para facilitar a tomada de decisões (dashboards, relatórios periódicos, etc)

Conta com ferramentas e tecnologias para:

- Coleta
- Apresentação
- Análise
- Auxílio na tomada de decisões



ARQUITETURA BÁSICA

ZABBIX

ZABBIX SERVER BACKEND

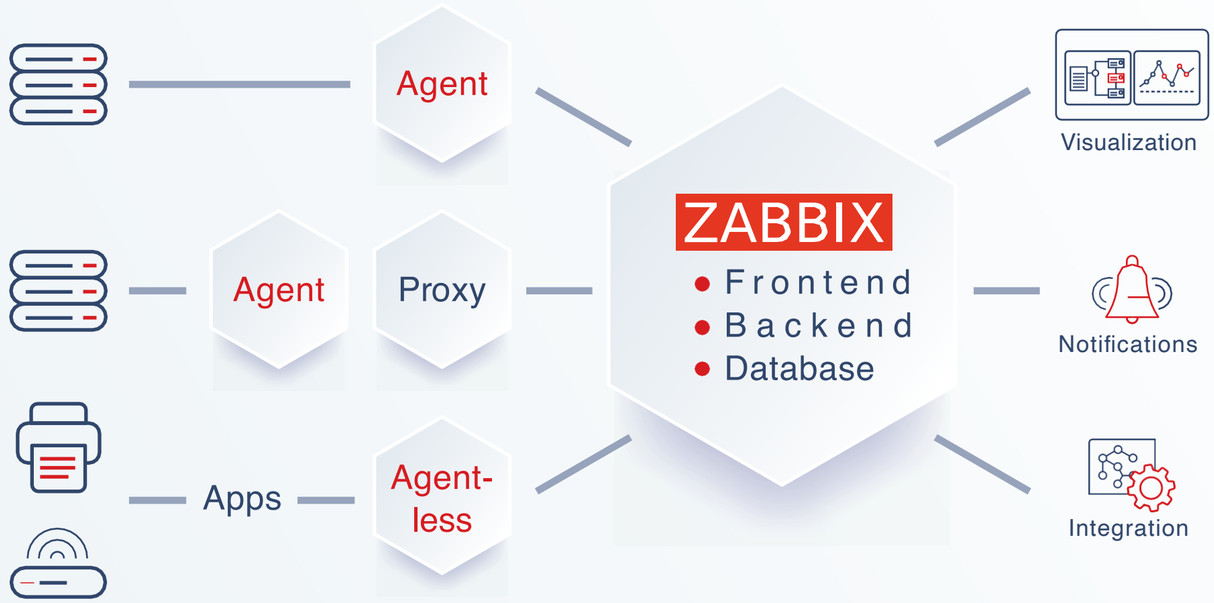
- Processo principal, responsável pela coleta e análise de dados
- Pode ser instalado em Linux, BSD, Raspbian e outros sistemas operacionais Unix-like
- Cluster de alta disponibilidade nativo do Zabbix server

DATABASE

- Armazena configurações e dados coletados
- PostgreSQL + TimescaleDB
- MySQL ou seus forks
- Oracle

FRONTEND

Aplicação PHP para realizar configuração e visualizar dados.

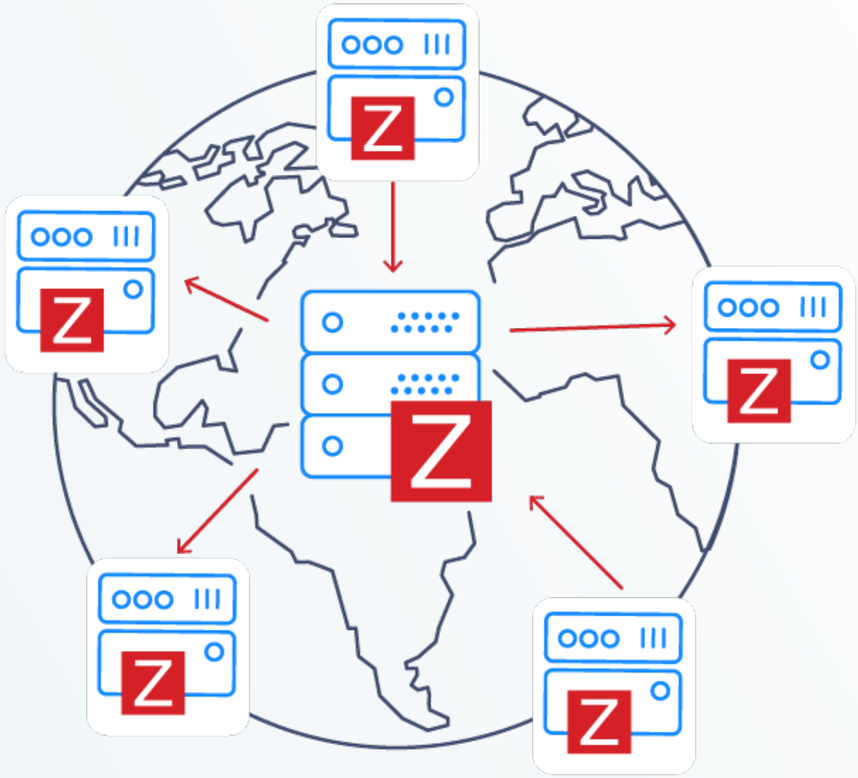


MONITORAMENTO DISTRIBUÍDO

ZABBIX

Zabbix proxies em locais remotos para redundância e fácil configuração

- Compressão de dados
- Monitoramento atrás de um firewall, DMZ
- Coleta de dados em caso de problema de rede
- Execução de scripts em hosts monitorados
- Controle de todos os proxies através de uma página

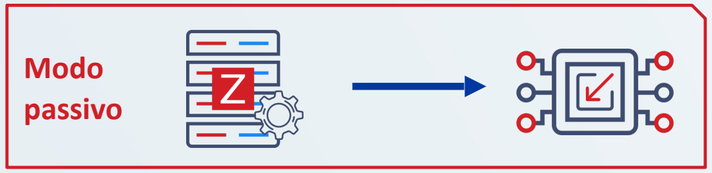


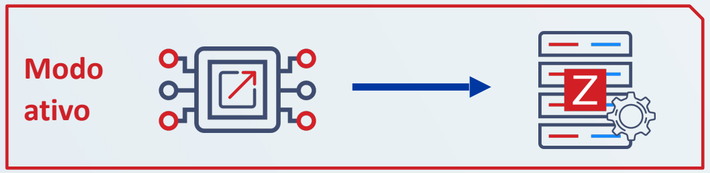
COLETA DOS DADOS

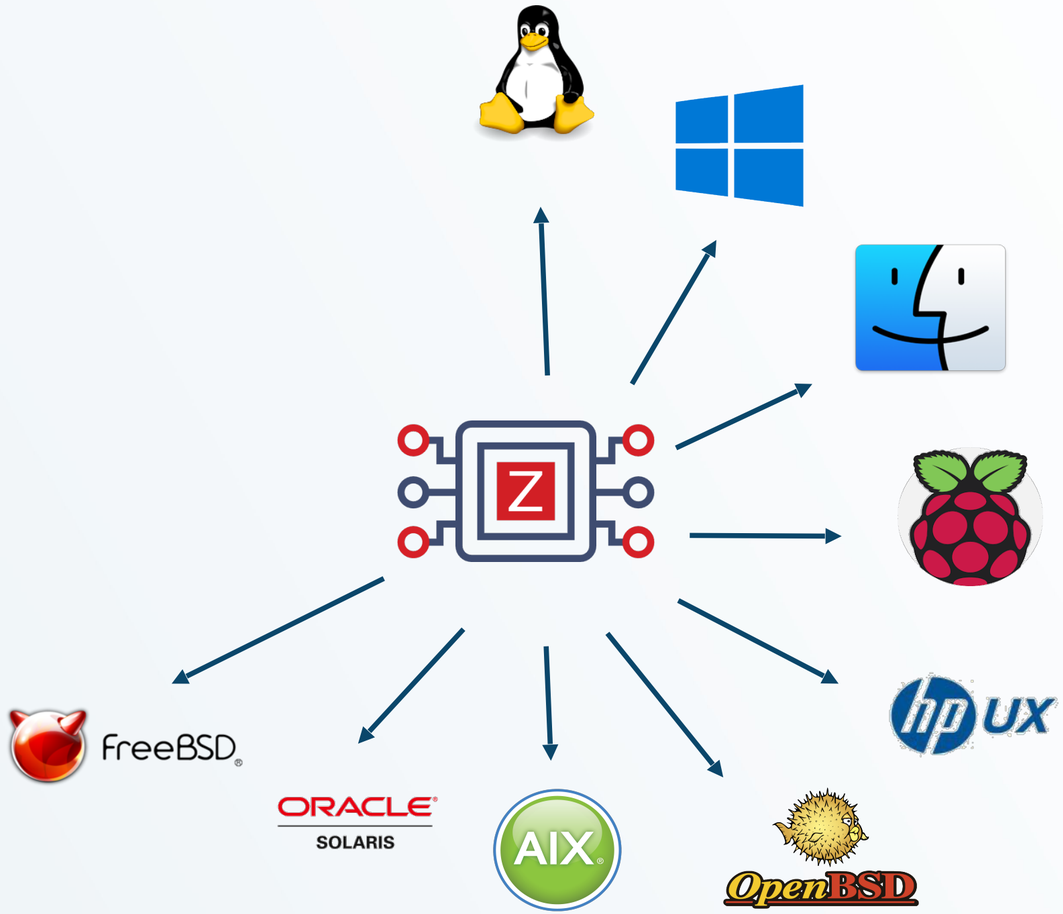
ZABBIX

Coleta com agente

- Pode rodar em várias plataformas
- Coleta dados de um dispositivo ou aplicação
- Baixo footprint de memória e uso de recursos
- Pode funcionar nos modos ativo e passivo (simultaneamente)
- Suporta comunicação encriptada e forma nativa







COLETA DOS DADOS

ZABBIX

Coleta sem agente

- Monitoramento é realizado diretamente pelo Zabbix server ou Proxy
- Coleta baseada em protocolos de redes:
  - Ping e verificação de portas
  - SNMP (v1, v2, v3)
  - HTTP
  - IPMI
  - SSH
  - Monitoramento de aplicações JAVA
  - Banco de dados via ODBC
  - Scripts customizados
  - Nem o céu é o limite…

COLETA DOS DADOS

ZABBIX

Coleta sem agente

- Monitoramento é realizado diretamente pelo Zabbix server ou Proxy
- Coleta baseada em protocolos de redes:
  - Ping e verificação de portas
  - **SNMP (v1, v2, v3)**
  - HTTP
  - IPMI
  - SSH
  - Monitoramento de aplicações JAVA
  - Banco de dados via ODBC
  - Scripts customizados
  - Nem o céu é o limite…

VISUALIZAÇÃO - DASHBOARDS

ZABBIX

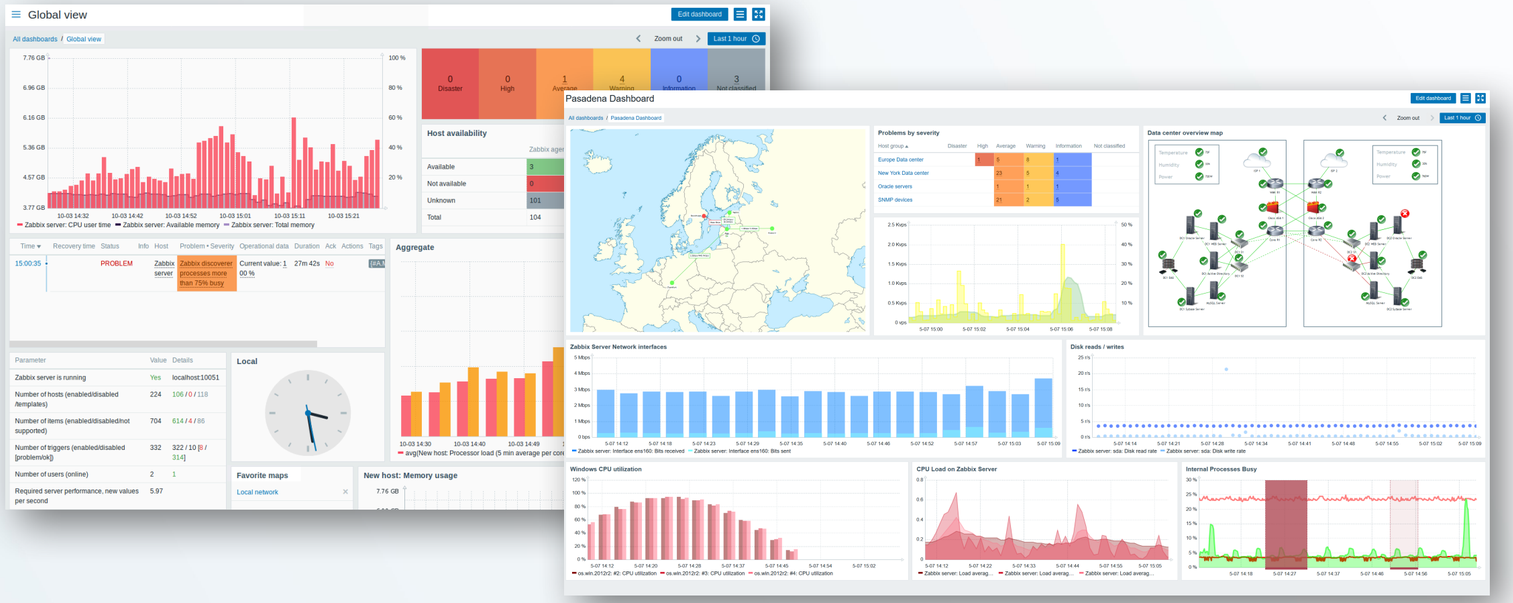
Através de Dashboards é possível visualizar um resumo de sua operação

Eles podem ter uma ou várias páginas, que podem ser rotacionadas em um Slide show de forma automática

Dashboards são baseados em widgets, pequenos painéis que trazem determinados tipos de informação

Exemplos de Widgets:

- Gráficos
- Mapas
- Valores isolados
- Resumo de problemas
- Relógio
- Entre outros...
- Personalizados



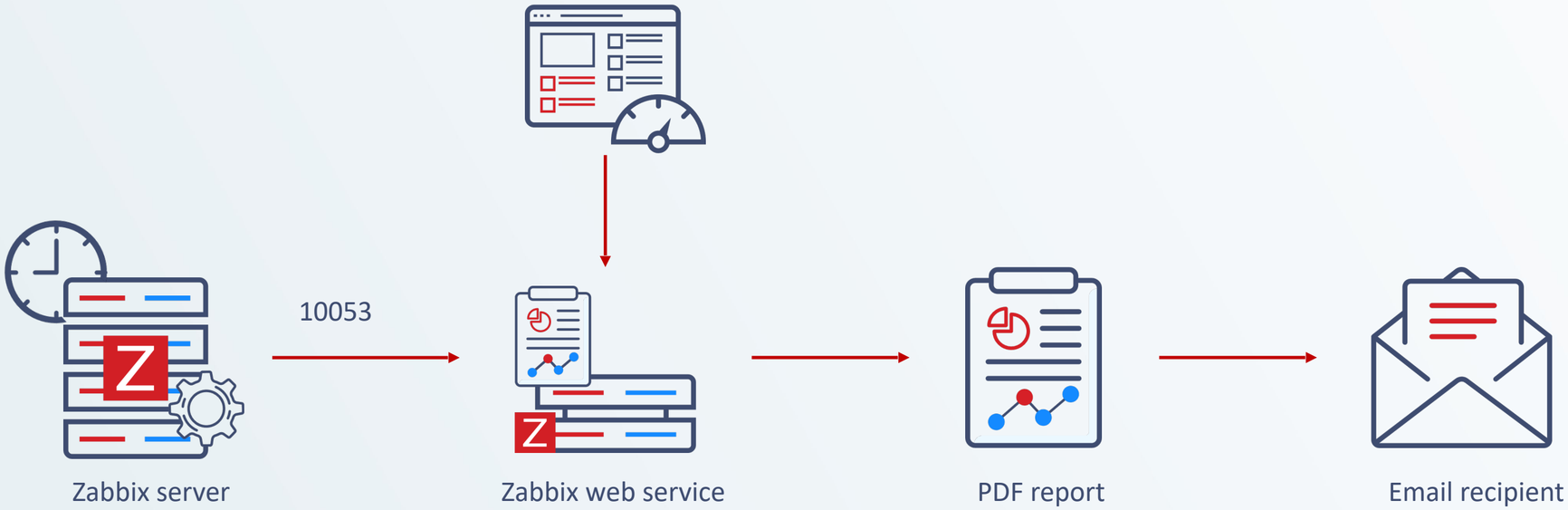
RELATÓRIOS AGENDADOS

ZABBIX

RELATÓRIOS EM PDF BASEADOS NOS DASHBOARDS

- Para dashboards com múltiplas páginas, apenas a primeira página pode ser usada no relatório

- Possibilita o envio não só para usuários do Zabbix, mas para endereços externos



MONITORAMENTO VIA SNMP

ZABBIX

ALGUNS PONTOS SOBRE O SNMP

- **S**imple **N**etwork **M**anagement **P**rotocol
- Coleta informações relacionadas à saúde e desempenho do dispositivo
- Operações suportadas:

Operação	Descrição da operação
GET	Retorna dados de um elemento presente em uma entidade da rede
GETNEXT	Retorna os dados subsequentes a um elemento de uma entidade da rede
SET	Envia configurações ou comandos de controle para uma entidade da rede
TRAP	Possibilita uma entidade da rede enviar notificações para a estação de gerência
INFORM	Uma trap reconhecida (a entidade da rede pode tentar reenviar a trap se nenhum reconhecimento for recebido (acknowledged trap))

MONITORAMENTO VIA SNMP

ZABBIX

ALGUNS PONTOS SOBRE O SNMP - VERSÕES

- **SNMPv1:**
  - Criado em meados dos anos 80
  - Fácil de configurar – Requer apenas uma string chamada “community“.
  - Muito vulnerável – informações são enviadas na rede em texto pleno
- **SNMPv2:**
  - Traz tudo o que a v1 tinha e inclui melhorias em performance, segurança e gerência
  - Introduz *GetBulkRequest*, comando *Inform* e suporte para contadores 64-bit
  - *Party-based security system* – muito complexo e amplamente não adotado 😢
  - SNMPv2c – Community-Based – Utiliza o esquema de segurança da v1
- **SNMPv3:**
  - Finalmente, segurança! x Mais complexo de configurar
  - Autenticação – para garantir que as mensagens sejam lidas apenas pelo recipiente desejado
  - Encriptação – Encripta as mensagens transferidas pela rede e garante que não possam ser lidas por usuários sem autorização

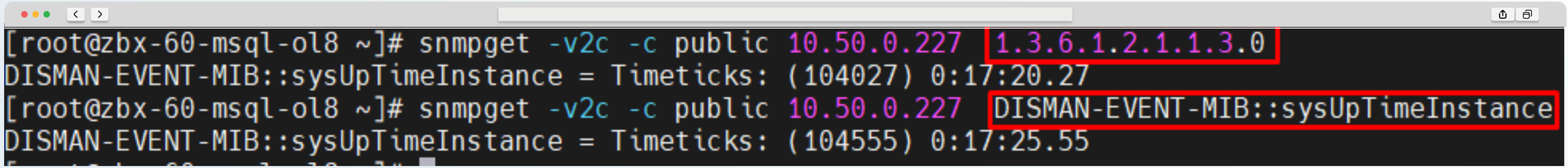
MONITORAMENTO VIA SNMP

ZABBIX

SUITE NET-SNMP

- É um pacote de ferramentas usadas para executar as operações do protocolo SNMP, e implementar SNMP v1, SNMP v2 e SNMP v3 utilizando IPv4 e IPv6

Operação	Comando	Descrição do comando
GET	snmpget	Utiliza a operação GET para retornar informações da entidade da rede
GETNEXT	snmpwalk	Utiliza a operação GETNEXT para consultar a árvore de informações de uma entidade da rede
SET	snmpset	Utiliza a operação SET para setar novas informações na entidade da rede
TRAP/INFORM	snmptrapd	Recebe e loga mensagens resultantes de operações TRAP e INFORM



MONITORAMENTO VIA SNMP

ZABBIX

MIB E OID

- **MIB = Management Information Base**
  - É um arquivo de texto com uma determinada formatação e organizado de forma hieráquica
  - Contem os detalhes dos **objetos** monitoráveis

- **OID = Object Identifier**
  - Endereço utilizado para diferenciar informações entre objetos
  - Representado por uma longa sequência de números separados por pontos

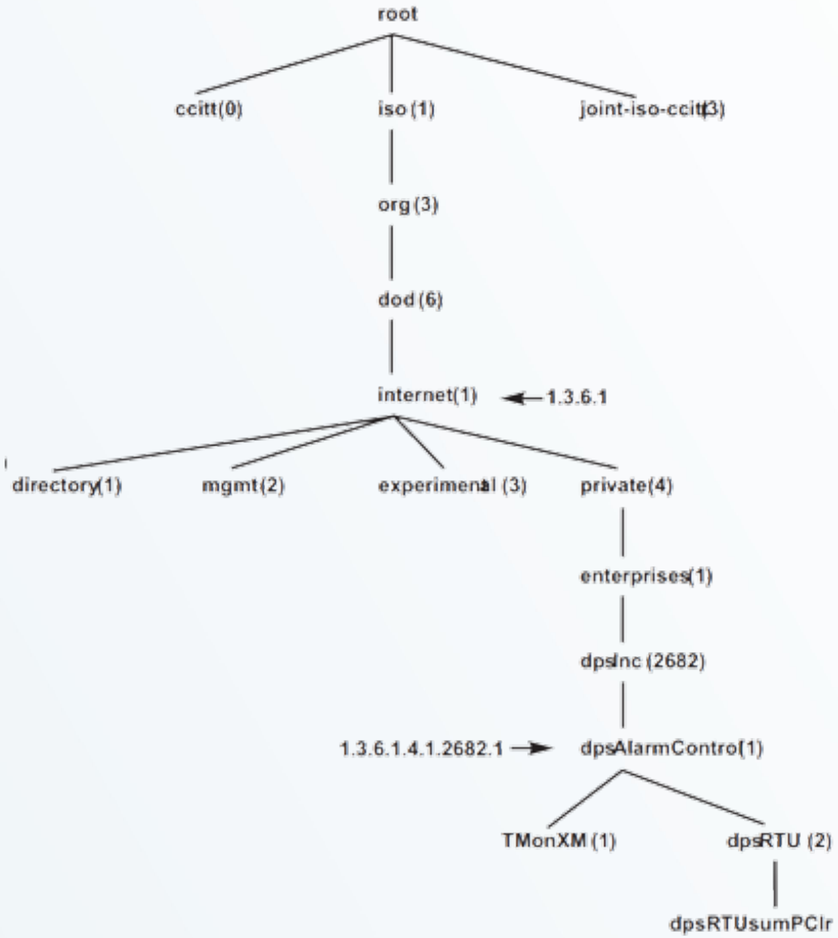
MONITORAMENTO VIA SNMP

ZABBIX

MIB E OID

- **MIB** = **M**anagement **I**nformation **B**ase
  - É um arquivo de texto com uma determinada formatação e organizado de forma hieráquica
  - Contem os detalhes dos **objetos** monitoráveis

- **OID** = **O**bject **Id**entifier
  - Endereço utilizado para diferenciar informações entre objetos
  - Representado por uma longa sequência de números separados por pontos



MONITORAMENTO VIA SNMP

ZABBIX

MIB E OID

- **MIB = M**anagement **I**nformation **B**ase
  - É um arquivo de texto com uma determinada formatação e organizado de forma hieráquica
  - Contem os detalhes dos **objetos** monitoráveis

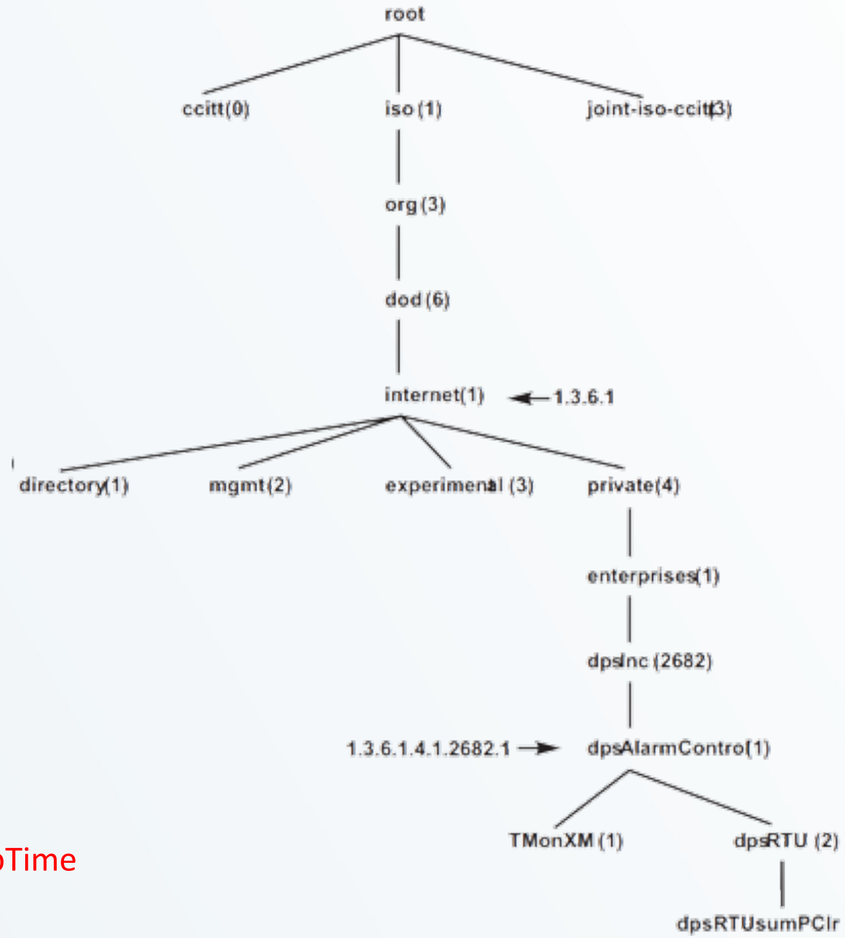
- **OID = O**bject **Id**entifier
  - Endereço utilizado para diferenciar informações entre objetos
  - Representado por uma longa sequência de números separados por pontos

.1	iso
.1.3	org
.1.3.6	dod
.1.3.6.1	internet
.1.3.6.1.2	mgmt
.1.3.6.1.2.1	mib-2
.1.3.6.1.2.1.1	system
.1.3.6.1.2.1.1.1	sysDescr
.1.3.6.1.2.1.1.2	sysObjectID
.1.3.6.1.2.1.1.3	sysUpTime

1.3.6.1.2.1.1.3

=

iso.org.dod.internet.mgmt.mib-2.system.sysUpTime



MONITORAMENTO VIA SNMP

ZABBIX

Zabbix x SNMP

- O Zabbix envia um request SNMP GET para o dispositivo
- O dispositivo responde com um valor ou uma mensagem de erro
- A comunicação por padrão se dá através do protocolo UDP na porta 161

OID	Name
1.3.6.1.2.1.1.1	sysDescr
1.3.6.1.2.1.1.2	sysObjectID
1.3.6.1.2.1.1.3	sysUpTime
1.3.6.1.2.1.1.4	**sysContact**
1.3.6.1.2.1.1.5	sysName
1.3.6.1.2.1.1.6	sysLocation

MONITORAMENTO VIA SNMP

ZABBIX

Zabbix x SNMPTrap

- Situações de problemas ou limiares são definidos no dispositivo
- Cada tipo de dispositivo tem seus itens de trap únicos
- Quando um problema é identificado, ele enviará a mensagem SNMP para todos os recipientes configurados

ZABBIX

PERGUNTAS?

ZABBIX