Utilizando Zabbix para Monitoramento de Infraestrutura de Redes

Uzias Manoel da Silva, Paulo Sérgio Gaudêncio Mauro, José Alexandre Ducatti

e-mail: uziasms@gmail.com; paulo.mauro@fatec.sp.gov.br; jose.ducatti@fatec.sp.gov.br

Faculdade de Tecnologia de São José do Rio Preto

Resumo: Este artigo tem como objetivo contribuir para gestão de monitoramento de infraestrutura de Tecnologia da Informação, apresentando um sistema de monitoramento de código aberto que auxiliará na integridade dos ambientes de tecnologia. O projeto foi estruturado através de uma virtualização, utilizando um servidor com sistema operacional Linux que para o funcionamento da ferramenta Zabbix foi necessário um serviço *web* (Apache), banco de dados *MySQL* e a linguagem de *Scripts PHP*. Para os dispositivos clientes foram usados uma máquina virtual com os sistemas operacional Windows 10 e duas com Ubuntu.

Palavras-chave: Monitoramento; Redes de computadores; Zabbix; Infraestrutura de Tecnologia da Informação; Cibersegurança; Gestão de servidores.

Abstract: *This article aims to contribute to the monitoring management of Information Technology infrastructure, presenting an open-source monitoring system that will help in the integrity of technology environments. The project was structured through virtualization, using a server with a Linux operating system that required a web server (Apache), SGBD MySQL and PHP Scripts language for the Zabbix tool to work. For client hosts, a machine with Windows 10 and another with Ubuntu Desktop was used.*

Keywords: *Monitoring; Computer network; Zabbix; Information Technology Infrastructure; cybersecurity; server management.*

1. INTRODUÇÃO

O administrador de sistemas de uma empresa está sempre sendo cobrado pelo seu gerente ou cliente, acerca das reclamações a respeito da disponibilidade dos servidores. Esse administrador costuma receber ligações noturnas após o seu horário de expediente, com relatos que serviços de T.I como servidores *web*, arquivo, banco de dados entre outros que estão "fora do ar". Com isso, tem uma grande geração de retrabalho, pois o administrador não consegue fazer o diagnóstico com agilidade do que ocorreu, a empresa acaba tendo que pagar os trabalhos extras e o administrador tem sua vida pessoal afetada.

Diante dessa situação é necessário atuar para uma solução definitiva, para isso um sistema de monitoramento é essencial, com ele é possível monitorar os dispositivos conectado à rede em tempo real, emitir relatórios sobre o consumo de recursos do sistema, verificar data e hora que um serviço parou e trabalhar de maneira preventiva e proativa na manutenção e *upgrade* dos dispositivos.

A ausência de monitoramento de rede pode resultar em vários prejuízos para as organizações, incluindo perda de dados, violações de segurança e tempo de inatividade prolongado, sendo que o valor e a credibilidade da organização estão associados a percepção que o cliente final tem das entregas de serviços e produtos.

2. JUSTIFICATIVA

Nota-se que a falta de monitoramento de rede pode resultar em prejuízos significativos para as organizações, incluindo perda de dados, violações de segurança e tempo

de inatividade prolongado e consequentemente perda financeira. É por isso que o monitoramento de rede é tão importante para garantir a segurança e a eficiência das operações das empresas.

3. OBJETIVO

Este trabalho apresenta a importância do monitoramento da infraestrutura de T.I nas organizações, e apresentar a ferramenta de monitoramento Zabbix, abordando como esta solução pode contribuir para a integridade e disponibilidade dos ambientes de tecnologia de informação, segurança da informação e tomada de decisão eficiente e proativa.

4. METODOLOGIA

A metodologia utilizada foi a consulta de livros, artigos, site oficial do Zabbix, fóruns, *Hypervison Oracle Virtual Box* para desenvolvimento do projeto e gestão com a ferramenta *Trello*.

Os *softwares* de monitoramento mais utilizados e concorrente do Zabbix são *PRTG Network Monitor* que possui licenciamento e *Nagios* de código aberto, o Zabbix foi escolhido para o desenvolvimento do projeto, pois é um software de código aberto com recursos nativos de estatísticas e também é um dos mais utilizados no Brasil e no mundo em comparação com os concorrentes mencionados.

5. TRABALHO SIMILARES

Conforme o corrente tema, encontramos outros trabalhos que citam as tecnologias que foi utilizada nesse projeto. Seguem-se alguns exemplos.

MONITORAMENTO E GERENCIAMENTO DE REDES UTILIZANDO ZABBIX, do pesquisador Washington Ernando Pereira Benício do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo. A monografia demonstra importância do monitoramento cujo objetivo é ser implantada na faculdade.

GESTÃO DA INFRAESTRUTURA DE TI COM ZABBIX, da pesquisadora Isamara F. Barbosa da Faculdade de Tecnologia do Estado de São Paulo, campus São José do Rio Preto. O artigo demonstra que as redes de computadores estão cada vez maiores e complexas, e a necessidade de monitoramento se tornou imprescindível para prevenção da indisponibilidade dos recursos de T.I.

6. MONITORAMENTO DE REDES E RECURSOS

O monitoramento de redes é de extrema importância para as organizações, pois permite que elas monitorem continuamente o tráfego de dados em suas redes e identifiquem problemas de desempenho ou segurança antes que eles se tornem problemas maiores.

A ausência de monitoramento de rede pode resultar em vários prejuízos para as organizações, incluindo perda de dados, violações de segurança e tempo de inatividade prolongado.

6.1 IMPACTOS NEGATICOS DA AUSÊNCIA DE MONITORAMENTO

Em 2019, a empresa de hospedagem *web* Hostinger sofreu uma violação de segurança que resultou na exposição de informações pessoais de mais de 14 milhões de clientes. A empresa afirmou que a violação ocorreu porque eles não monitoraram seus sistemas de forma adequada e, como resultado, não detectaram a violação até que já fosse tarde demais (ZDNet, 2019).

Em 2017, o site de comércio eletrônico Amazon sofreu um problema de rede que resultou em tempo de inatividade prolongado para muitos de seus clientes. A empresa afirmou que o problema ocorreu porque eles não monitoraram suas redes de forma adequada e, como resultado, não detectaram o problema até que já fosse tarde demais. O tempo de inatividade resultou em perda de receita e danos à reputação da empresa (Forbes, 2019).

7. ZABBIX

O Zabbix é um *software* de monitoramento de redes de código aberto, desenvolvido para gerenciar redes e oferecer uma visão abrangente dos dispositivos, aplicativos e serviços que compõem a infraestrutura de T.I das organizações.

Com o Zabbix, é possível monitorar o desempenho da rede em tempo real, coletar informações sobre a disponibilidade dos dispositivos de rede tais como servidores, *switches*, roteadores, impressoras e outros, analisar históricos de monitoramento, gerar relatórios personalizados, configurar ações automatizadas como comandos remotos e notificação para os usuários, integrar com outros sistemas de gerenciamento de T.I e alertar sobre possíveis problemas antes que eles se tornem críticos (ZABBIX, s/d).

8.1 COMO SURGIU

A ideia surgiu em 1998, pelo administrador de sistema Alexei Vladishev que trabalhava em um banco da Letônia, pois não estava satisfeito com os sistemas que trabalhava na época. Em 2005 foi fundado a empresa Zabbix SIA, após o lançamento da versão 1.0 do Zabbix. Atualmente, a versão do Zabbix é a Zabbix 6.4 que foi lançada em 7 de março de 2023. A Zabbix possui escritórios na Europa, Estados Unidos, Japão e América Latina (ZABBIX, s/d).

8.2 ARQUITETURA

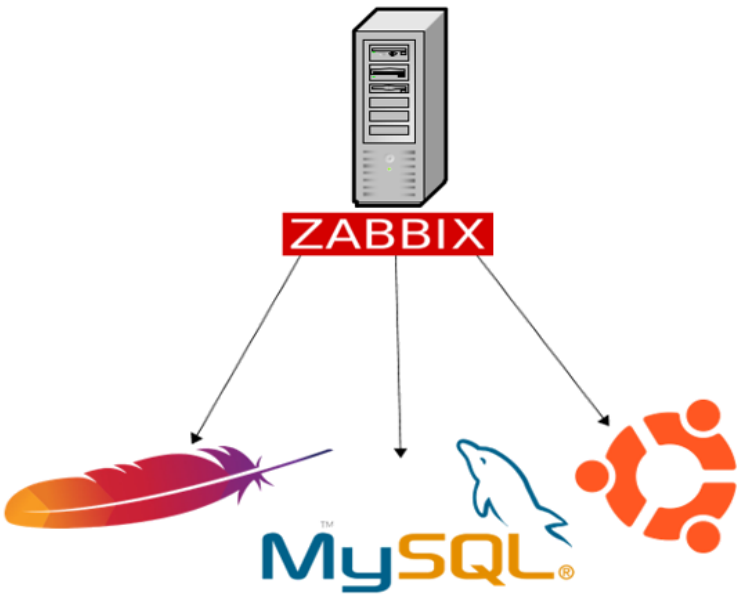
A arquitetura do Zabbix é baseada, dentro do contexto dos serviços de rede, no modelo *three-tier*, que faz uma abordagem em três camadas. Essas camadas são: a aplicação, o banco de dados e a interface *web*.

A camada de aplicação é representada pelo *back-end*, responsável por fazer a coleta dos dados nos ativos de rede. A camada de banco de dados é representada pela base de dados, que fica responsável por armazenar as informações coletadas pelo *back-end* e apresentá-las ao *front-end*. Já a camada de interface *web* é representada pelo *front-end*, que dá acesso a informações de monitoramento aos usuários que utilizam o Zabbix.

O *back-end* do Zabbix foi desenvolvido com a linguagem C e o *front-end* em PHP (LIMA, 2014).

A Figura 1 exibe a arquitetura utilizada no formato *Single Server* (Servidor único), na qual é utilizado o sistema operacional Linux Ubuntu para instalação das aplicações Zabbix, banco de dados e serviço *web*.

Figura 1: Arquitetura do Zabbix Single *Server*



Fonte: Elaborado pelo autor.

8.3 COMPONENTES DO ZABBIX

Para compreender o funcionamento do software Zabbix faz-se necessário o conhecimento de alguns componentes que compõem o software, os principais são Zabbix *Server*, Zabbix *Proxy*, Zabbix *Agent*, Gestão de Acesso, *Hosts*, Grupos de *Hosts*, Itens, *Triggers*, *Templates*, Mídias e Notificações, Ações, Autorregistro de *Hosts*, Comandos Remotos, *Tags*, Monitoramento, *Dashboards* e Auditoria. Todos serão explicados a seguir.

8.3.1 ZABBIX SERVER

Zabbix *Server*, é um processo central do *software* Zabbix que executa e faz o monitoramento, interagindo com os Zabbix *Proxies* e Agentes, calcula *triggers*, envia notificações sendo um repositório central de dados. Este serviço é suportado nos sistemas operacionais: Linux, Solaris, AIX, HP-UX, Mac OS X, FreeBSD, OpenBSD, NetBSD, SCO Open *Server* e Tru64/OSF1 (Zabbix, s/d).

8.3.2 ZABBIX PROXY

É um recurso opcional que pode coletar dados em nome do Zabbix *Server*, diminuindo a carga de processamento do *Server*. O *hardware* do Zabbix *Proxy* não precisa ter o mesmo desempenho do *Server*, e para o seu funcionamento é necessário a instalação de um banco de dados que tem suporte para os SGBDs SQLite, MySQL, PostgreSQL e outros. Este serviço é suportado nos sistemas operacionais: Linux, Solaris, AIX, HP-UX, Mac OS X, FreeBSD, OpenBSD, NetBSD, SCO Open *Server*, Tru64/OSF1 (Zabbix, s/d).

8.3.3 ZABBIX AGENT

É um processo implementado nos alvos de monitoramento, para monitorar ativamente os recursos e aplicações locais tais como (discos e partições, memória, estatísticas do processador etc.), que reporta para o Zabbix *Server* ou Zabbix *Proxy*. Este serviço é suportado nos sistemas operacionais: Linux, IBM AIX, FreeBSD, NetBSD, OpenBSD, HP-UX, Mac OS X, Solaris: 9, 10, 11, Windows: 2000, XP, 7, 8, 10, Vista, *Server* 2003, 2008. (Zabbix, s/d).

8.3.4 GESTÃO DE ACESSO

A gestão de acesso do Zabbix possui usuários, grupos e *roles* (permissão de acesso). Os usuários, devem possuir um nome único para se conectar a interface *web* do Zabbix, as credenciais são criptografadas e o usuários do Zabbix são separados dos usuários do sistema operacional onde está sendo hospedado o servidor Zabbix.

Os grupos de usuários, são criados para organizar equipes/funções, no Zabbix existem alguns grupos pré-definidos e a possibilidade de criação e alteração.

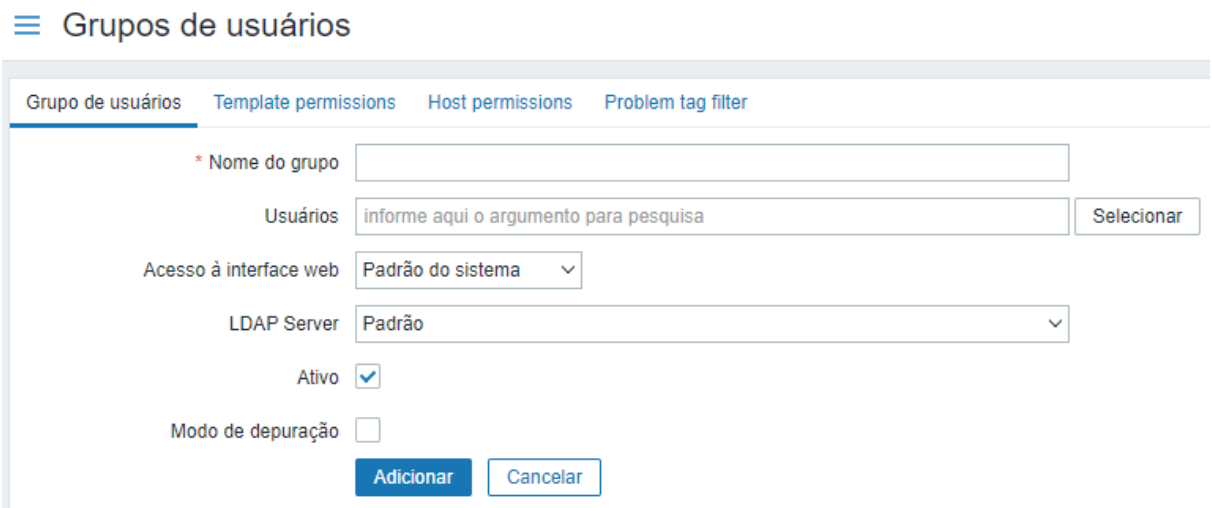
As *Roles* (Permissão de acesso), servem para gerenciar o acesso dos usuários e grupos, nestas configurações incluem criação de usuário, visualização de gráficos, alerta críticos entre outros, o Zabbix possui *roles* nativas.

O Fluxo para administração é criar as *roles* e grupos e depois associá-la aos usuários.

O Zabbix também oferece suporte à autenticação *LDAP* e *Active Directory*, o que permite que o administrador de sistema integre facilmente o gerenciamento de usuários e permissões com seu diretório corporativo (Zabbix, s/d).

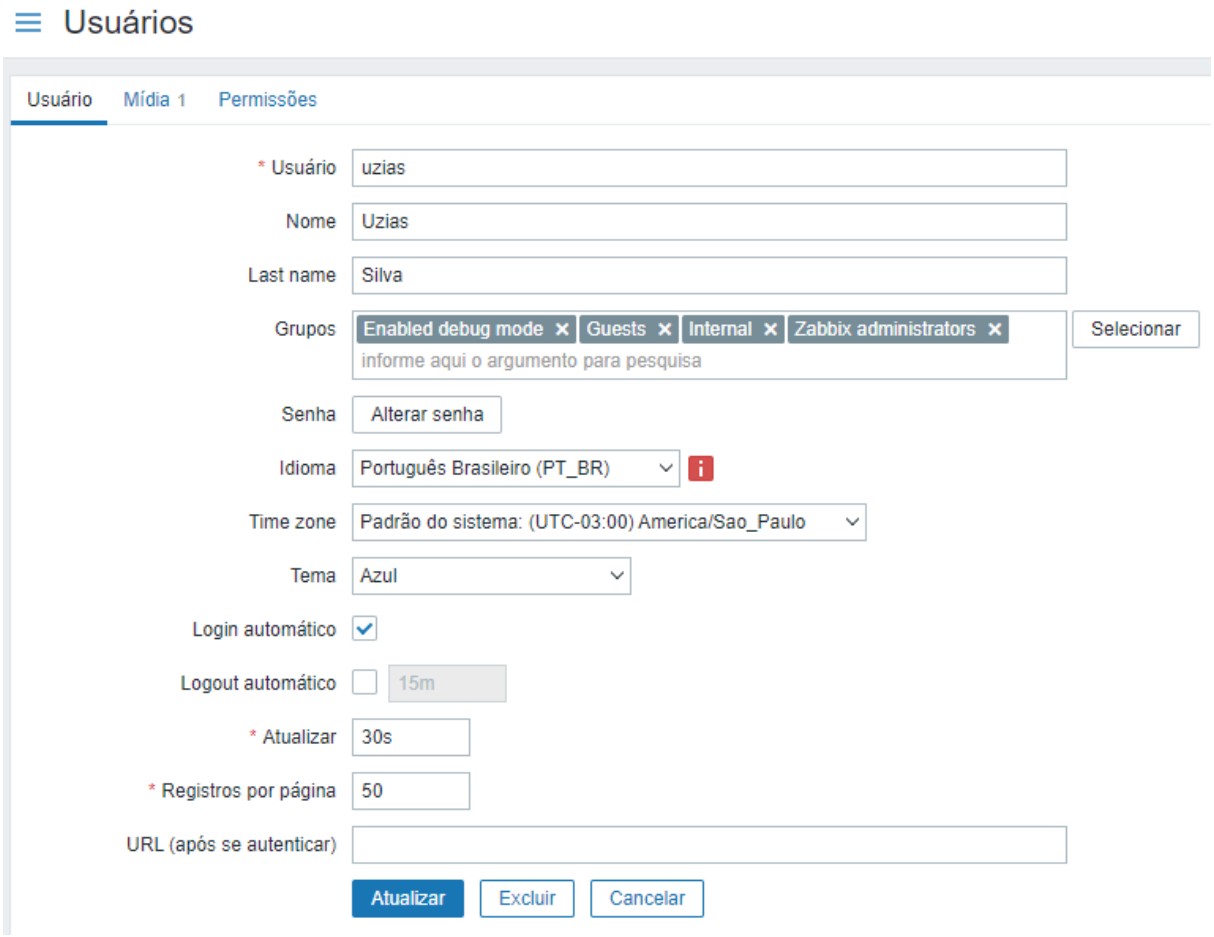
A Figura 2, abaixo, contém os campos necessários para criação de Grupos de Usuários e a Figura 3, os campos de Usuários.

Figura 2: Criação Grupos de usuários



Fonte: Elaborado pelo autor.

Figura 3: Criação de usuários



Fonte: Elaborado pelo autor.

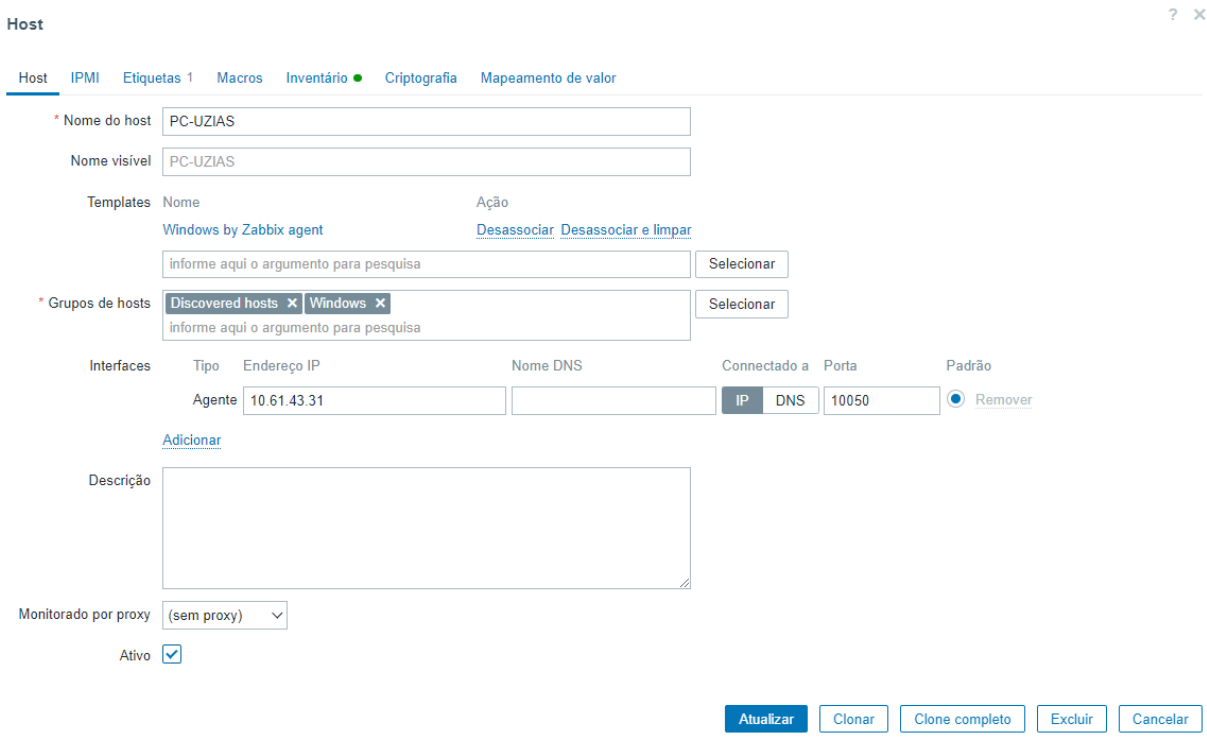
8.3.5 HOSTS

Os *hosts*, são todos os dispositivos que deseja fazer o monitoramento, pode ser qualquer dispositivo conectado à rede tais como servidores, impressoras, roteadores, *switches* etc. Pode ser criado manual e automaticamente via configurações do agente.

Os *Hosts* são associados ao servidor Zabbix ou *proxy*, também é possível clonar um *host*, para facilitação do gerenciamento dos *hosts* (Zabbix, s/d).

A Figura 4 contém os campos de configuração de um *host* de monitoramento entre eles o nome do *host*, *templates* associados, grupo que pertence, interface que está sendo utilizada (protocolo, IP e porta) e se existe um *proxy*.

Figura 4: Campos de Configuração de *Host*



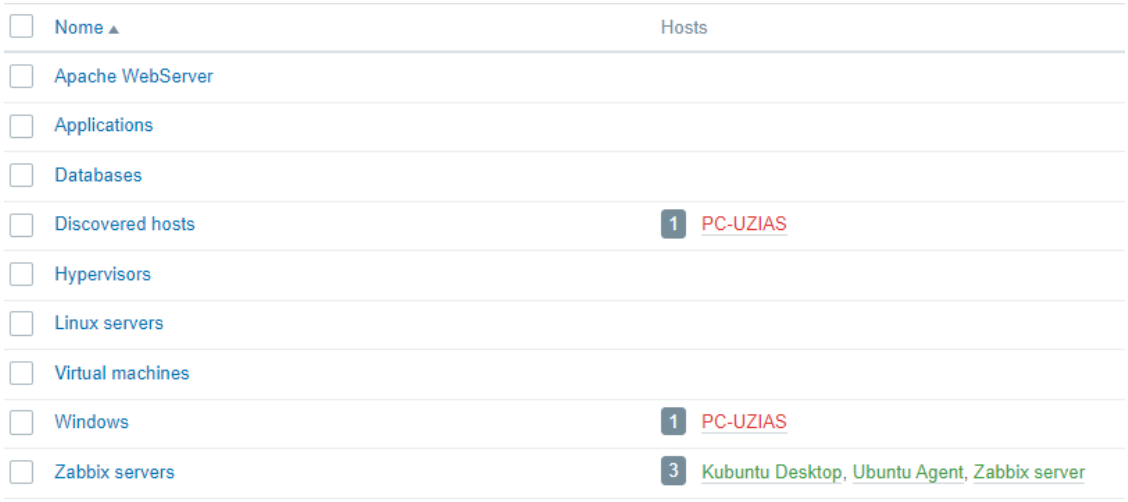
Fonte: Elaborado pelo autor

8.3.6 GRUPOS DE HOSTS

São usados para organizar os *hosts* que possuem características comuns, por exemplos servidores Linux, *Web*, Banco de Dados etc. Os grupos podem ser usados para medir disponibilidade de um serviço (Zabbix, s/d).

A Figura 5 contém os grupos de *hosts* e membros e a Figura 6 campo para criação de grupos de *hosts*.

Figura 5: Listagem Grupos de *Hosts* e membros



Fonte: Elaborado pelo autor

Figura 6: Criação Grupo de Hosts

Fonte: Elaborado pelo autor.

8.3.7 ITENS

São instrução de coleta de métrica a um *host* por exemplo, consumo de memória *RAM*, espaço em disco, porcentagem de uso do processador entre outros. O Zabbix oferece vários tipos de itens de monitoramento, incluindo *Zabbix Agent*, *Simple Check*, *SNMP*, *SSH* entre outros.

Estes itens retornam informações do tipo numérico, texto, *log* e caractere, informando a condição do *host* monitorado. Os itens também precisam de um intervalo de atualização que pode ser em segundos, minutos, horas e no máximo 1 dia. O Zabbix permite escolher a unidade de medida Megabytes, Gigabyte etc.

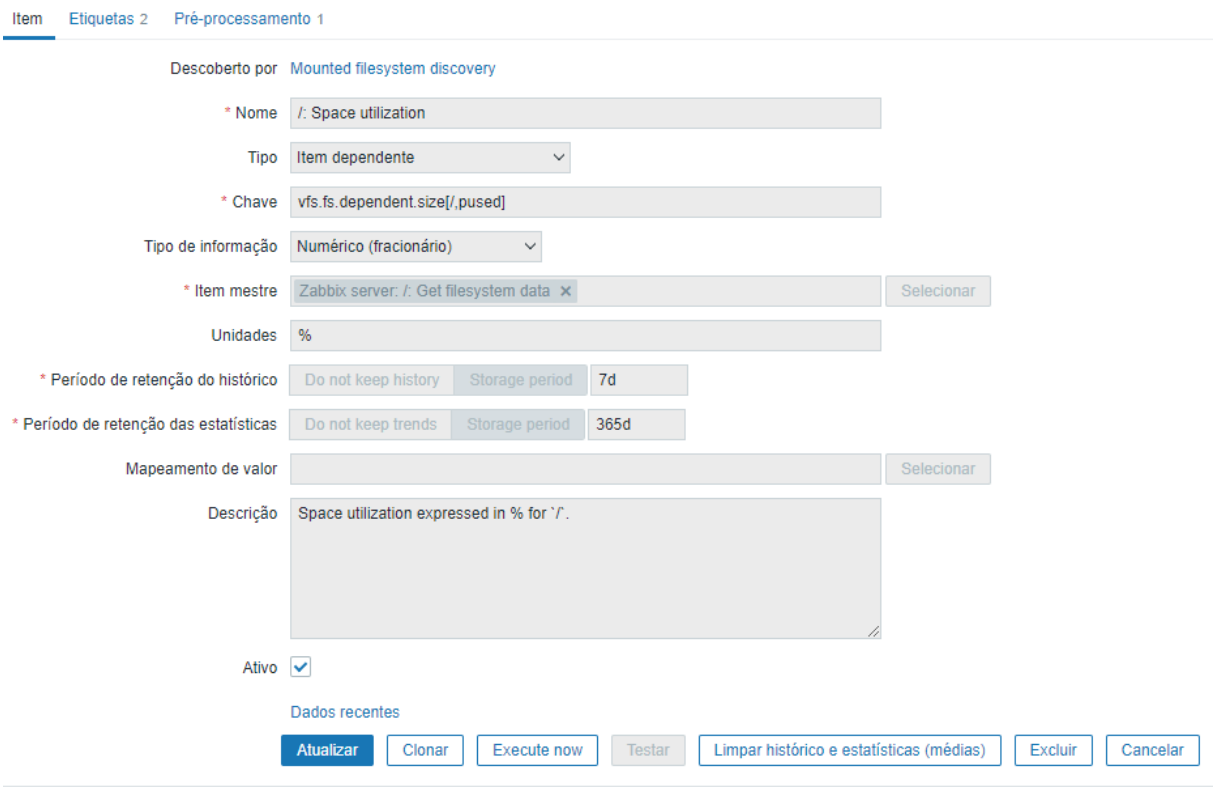
Na configuração dos Itens, é possível configurar o prazo de histórico de armazenamento do *host* coletado.

Histórico de tendência, dentro do intervalo de uma hora o Zabbix mostra o valor mínimo, médio e máximo coletado. A ferramenta possibilita configurar o período de histórico que a tendência ficará armazenado.

Caso não encontre nenhum item na lista, o Zabbix permite customização, porém só é aplicável a monitoramento com o agente instalado (Zabbix, s/d).

A Figura 7 exibe as configurações do Item que verifica a porcentagem de uso, da partição / do sistema operacional, onde está sendo hospedado o Zabbix *Server*.

Figura 7: Item, porcentagem de uso da partição / do servidor Zabbix



Fonte: Elaborado pelo autor

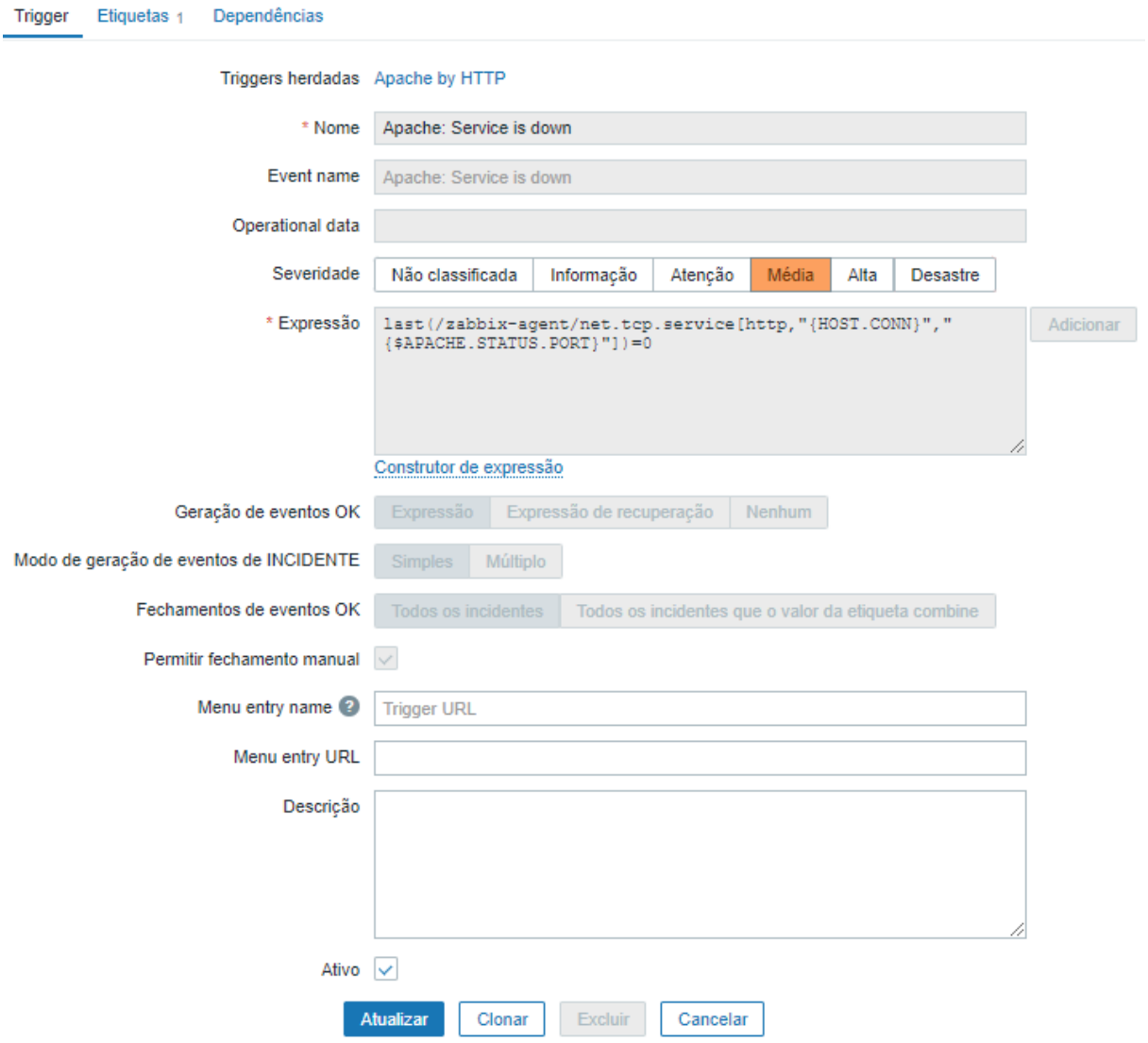
8.3.8 TRIGGERS

Triggers ou Gatilhos, são elementos que avaliam um item de monitoramento coletado, por exemplo, o serviço *web* deixou de funcionar.

Processo, dado recebido do item é feito avaliação da normalidade, se estiver dentro da normalidade o *status* será “OK”, caso contrário *status* será “PROBLEMA”, dado o *status* em problema o *trigger* abre um incidente e atribui um nível de severidade ao problema que são eles (Não Classificada, Informação, Atenção, Média, Alta e Desastre). Os *triggers* podem ser a base da execução de uma ação, tais como disparo de notificações via *Telegram*, E-mail, SMS ou comandos remotos para tentativa de resolver o problema (Zabbix, s/d).

A Figura 8 exibe as configurações de um *trigger* que verifica a disponibilidade do serviço Apache, entre os dados exibidos estão, o nome do *trigger* e evento, nível de severidade e expressão lógica que verifica se a porta *HTTP* 80 está inativa.

Figura 8: *Trigger* Serviço Apache parado.



Fonte: Elaborado pelo autor.

8.3.9 TEMPLATES

Os *templates* no Zabbix são modelos predefinidos de configuração que contêm itens de monitoramento, *triggers*, gráficos, *dashboards* e outras. Os *templates* são especialmente úteis para cenários em que é preciso monitorar muitos *hosts* que possuem as mesmas configurações.

Em vez de configurar cada *host* individualmente, o usuário pode associar um *template* com as configurações necessárias e aplicá-lo a todos os *hosts* ou grupo de *hosts* relevantes. Isso economiza tempo e minimiza o risco de erro humano na configuração manual.
Existem diversos *templates* nativos do Zabbix, também é possível importar e exportar e associar um *template* a outro, por exemplo, existem características semelhantes de vários *hosts* que estão sendo monitorados, que são sistemas operacionais Linux com serviço *web Apache*, o usuário pode criar um *template* e associar os *templates Apache by HTTP e Linux by*

Zabbix agent, desta forma terá um *template* centralizado e aumentaria a produtividade. No site oficial Zabbix possui uma comunidade onde os usuários conseguem compartilhar seus *templates* (Zabbix, s/d).

A Figura 9 exibe o conjunto de conteúdo que possui um *template* e a quantidade

Figura 9: Conteúdos de *templates*

Nome ▲	Hosts	Itens	Triggers	Gráficos	Dashboards	Descoberta	Web	Fornecedor	Version
Windows by SNMP	Hosts	Itens 13	Triggers 7	Gráficos 1	Dashboards 2	Descoberta 3	Web	Zabbix	6.4-0
Windows by Zabbix agent	Hosts 1	Itens 34	Triggers 13	Gráficos 5	Dashboards 2	Descoberta 4	Web	Zabbix	6.4-0

Fonte: Elaborado pelo autor.

8.3.10 MÍDIAS E NOTIFICAÇÕES

O Zabbix, oferece notificações para informar aos usuários quando ocorrem eventos ou problema de monitoramento. As notificações podem ser enviadas por vários meios, como e-mail, SMS, *Telegram*, *Microsoft Teams* e outros, permitindo que os usuários saibam imediatamente sobre problemas em seu ambiente de monitoramento. É possível usar *templates* existentes de notificação ou criar. O Processo é, criar a mídia e associar aos usuários (Zabbix, s/d).

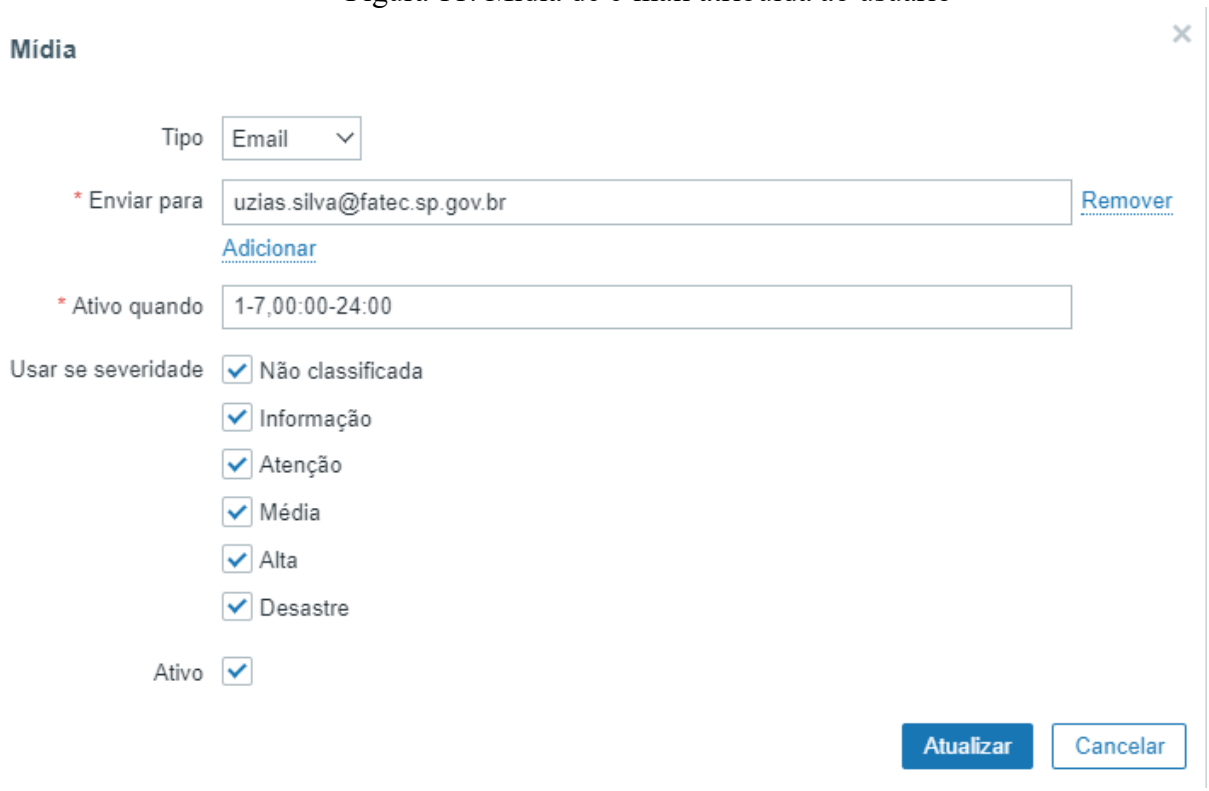
A Figura 10 lista as mídias disponíveis e a Figura 11 contém as informações necessárias para atribuição de uma mídia ao usuário.

Figura 10: Mídias disponíveis

Nome ▲	Tipo	Status	Usado nas ações	Detalhes
Brevis.one	Webhook	Inativo		
Discord	Webhook	Inativo		
Email	E-mail	Ativo		Servidor SMTP: "smtp.office365.com", email: "uzias.silva@fatec.sp.gov.br"
Email (HTML)	E-mail	Inativo		Servidor SMTP: "mail.example.com", SMTP helo: "example.com", email: "zabbix@example.com"
Express.ms	Webhook	Inativo		
Github	Webhook	Inativo		
GLPi	Webhook	Inativo		
Gmail	E-mail	Inativo		Servidor SMTP: "smtp.gmail.com", email: "zabbix@example.com"

Fonte: Elaborado pelo autor.

Figura 11: Mídia de e-mail atribuída ao usuário



Fonte: Elaborado pelo autor.

8.3.11 AÇÕES

As ações no Zabbix são mecanismos para automatizar a resposta a eventos, *triggers* e alertas gerados pelo sistema de monitoramento. As ações podem ser configuradas para realizar diversas tarefas, como enviar notificações, executar *scripts* personalizados, silenciar alertas, criar *tickets* de suporte, entre outros.

As ações mais utilizadas são, 1) eventos de *triggers*, quando abre um incidente *status* (PROBLEMA) ou Recuperação (OK), 2) evento de descoberta quando um ativo é encontrado na rede, 3) evento de autorregistro quando é recebido uma solicitação de autorregistro, 4) eventos internos e quando itens ou *triggers* não são suportados ou possuem o *status* desconhecido (Zabbix, s/d).

8.3.12 AUTORREGISTRO DE HOSTS

O autorregistro de *hosts* no Zabbix permite que os *hosts* sejam automaticamente adicionados ao sistema de monitoramento. O pré-requisito para o funcionamento é ter o Zabbix Agente instalado, após este processo, o arquivo de configuração do agente deve ser ajustado para autorregistro.

Após a configuração no *Hosts*, na interface *web* do servidor Zabbix, é preciso habilitar a ação de autorregistro de *hosts* e criar a ação. No processo de criação da ação é possível adicionar *templates* e grupos de *hosts* nos *hosts* que serão cadastrados automaticamente (Zabbix, s/d).

8.3.13 COMANDOS REMOTOS

Os comandos remotos são uma funcionalidade do Zabbix que permite que execute comandos em *hosts* remotos diretamente do servidor Zabbix ou Zabbix *Proxy* de forma proativa em caso de falha de um serviço, estes comandos são configurados no elemento de ações, alguns exemplos de comandos remotos são: recuperar um serviço que caiu, liberar espaço em disco antes que o servidor pare entre outros.

Para o funcionamento é necessário ter a permissão de usuário e *firewall* para que o Zabbix atue (Zabbix, s/d).

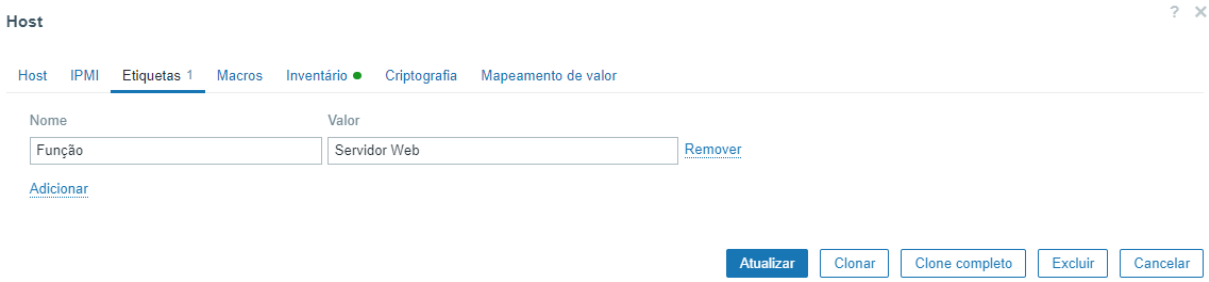
8.3.14 TAGS

As *tags* ou etiquetas, são uma funcionalidade que permite que o usuário adicione metadados personalizados aos seus *hosts*, *triggers* e outros objetos de monitoramento. Isso pode ser útil para organizar e categorizar seus objetos de monitoramento de maneira mais eficiente e para facilitar a pesquisa e o agrupamento desses objetos.

As etiquetas podem ser adicionadas aos objetos de monitoramento durante a criação ou edição de um *host*, *trigger* ou outro objeto no Zabbix. Cada etiqueta consiste em um par chave-valor, onde a chave é um nome descritivo para a etiqueta e o valor é um valor opcional que pode ser usado para filtrar e agrupar objetos (Zabbix, s/d).

A Figura 12 exibe a configuração de uma etiqueta em um *host*.

Figura 12: Etiqueta atribuída a um *Host*



Fonte: Elaborado pelo autor.

8.3.15 MONITORAMENTO E DASHBOARDS

No menu monitoramento são exibidos os dados que o Zabbix está configurado para coletar, visualizar e agir. O submenu *Hosts* que está dentro do menu monitoramento, exibe uma lista completa de *hosts* monitorados com informações detalhadas sobre o nome do *host*, interface do *host*, disponibilidade, etiquetas, problemas atuais, status (ativado/desativado) e *links* para navegar até os dados mais recentes do *host*, histórico de problemas, gráficos, painéis e cenários da *web*, abaixo descrição das colunas:

• Nome: Exibe o nome do *host* visível.

• Interface: Exibe a interface principal (IP e Porta associado para o monitoramento).

• Disponibilidade: Exibe ícones que representam os tipos de interface (Agente Zabbix, *SNMP, IPMI e JMX*) representados por *status* que classifica as disponibilidades por cores que

são: verde: todas interfaces disponíveis, amarelo: pelo menos uma interface disponível e pelo menos uma indisponível, vermelho: nenhuma interface disponível e por fim cinza: pelo menos uma interface desconhecida (nenhuma indisponível).

• Etiquetas: Etiquetas do *host* e todos os modelos vinculados, com macros não resolvidas.

• Status: Exibe o *status* do *host*, Ativado ou Desativado.

• Dados recentes: Clicar no *link* abrirá a página Monitoramento - Últimos dados com todos os dados mais recentes coletados do *host*.

• Problemas: O número de problemas de *host* abertos classificados por gravidade. A cor do quadrado indica a gravidade do problema. O número no quadrado significa o número de problemas para determinada gravidade.

• Gráficos: Clicar no *link* exibirá os gráficos configurados para o *host*.

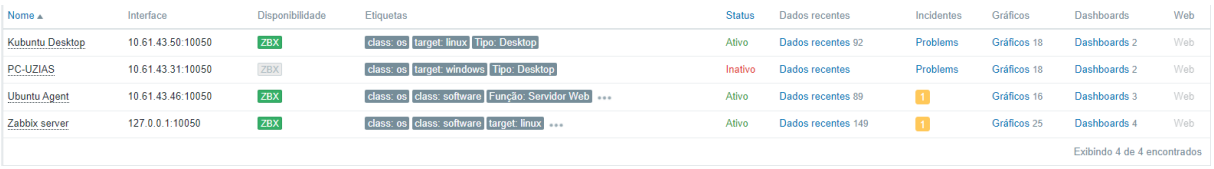
• *Dashboard*: Clicar no *link* exibirá os *dashboards* configurados para o *host*.

• *Web*: Clicar no *link* exibirá cenários da *web* configurados para o *host*

A ferramenta permite a filtragem de um *host* monitorado por nome, grupos de *hosts*, *IP, DNS*, porta, severidade, status e etiquetas (Zabbix, s/d).

A Figura 13 exibe as informações gerais dos *hosts* que estão sendo monitorados

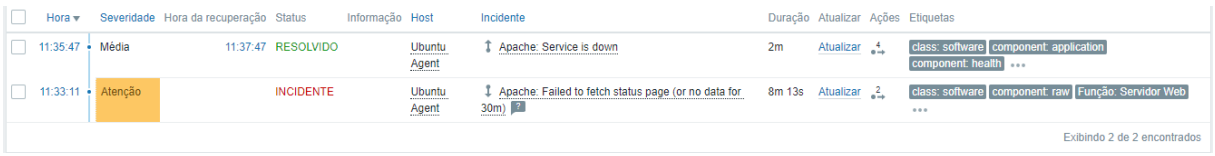
Figura 13: Monitoramento de *Hosts*



Fonte: Elaborado pelo autor.

A figura 14 exibe as informações de um Incidente que ocorreu.

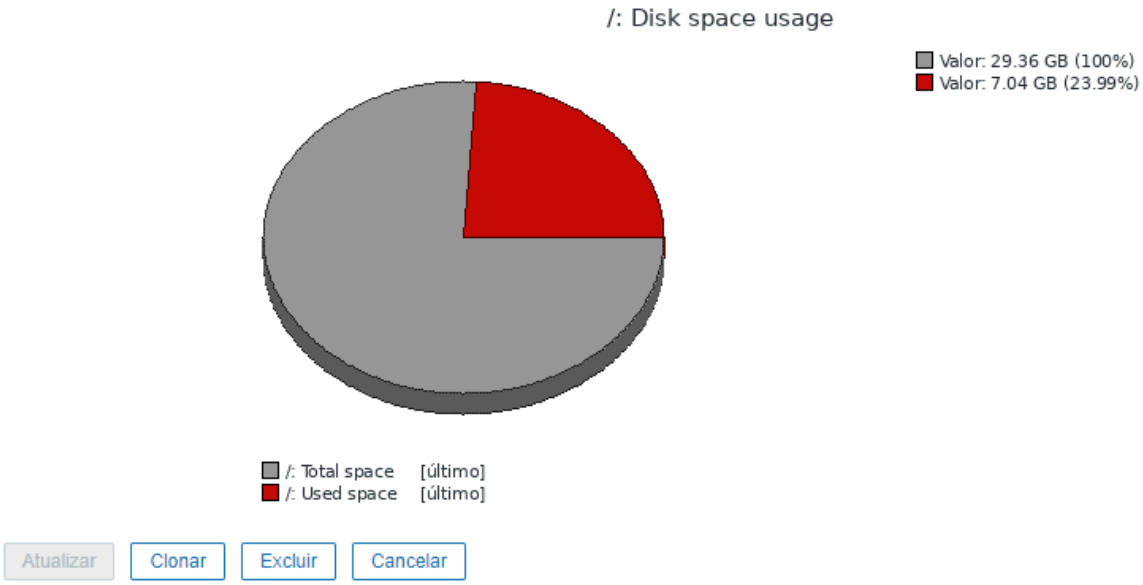
Figura 14: Incidente de *Host*



Fonte: Elaborado pelo autor.

A Figura 15 exibe o gráfico, referente a porcentagem de uso da partição barra do servidor zabbix.

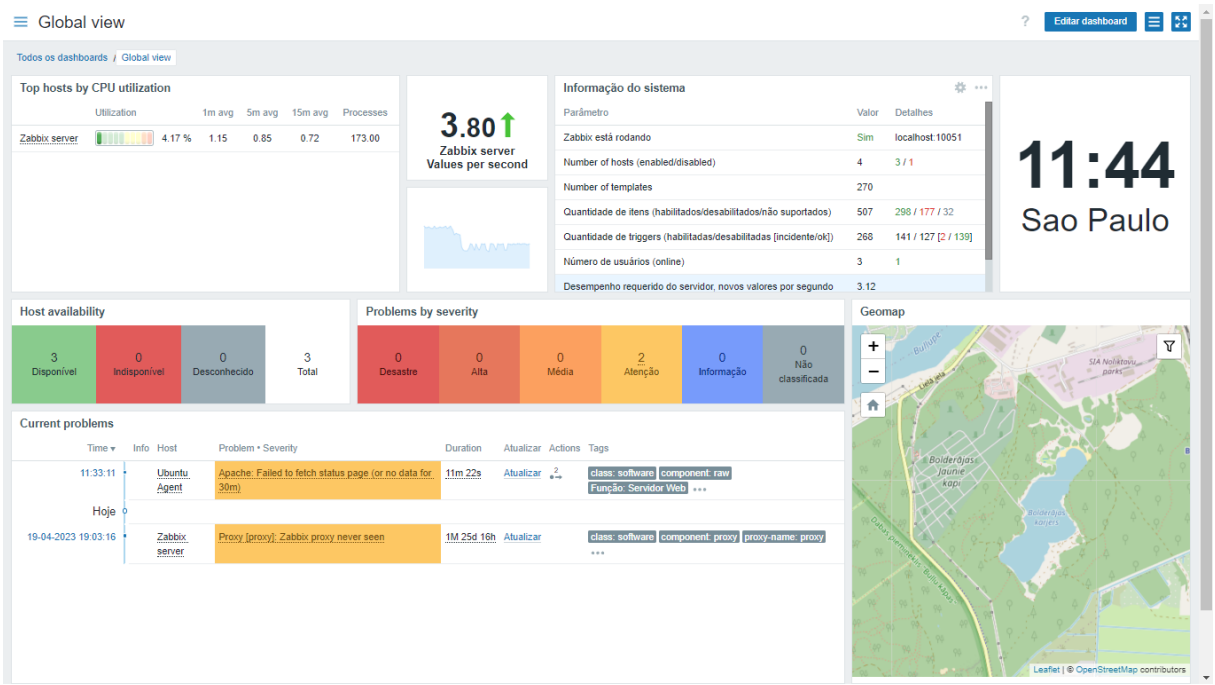
Figura 15: Gráfico utilização da partição /



Fonte: Elaborado pelo autor.

A Figura 16 exibe o *dashboard* principal do Zabbix, listando informações gerais do ambiente monitorado tais como utilização da CPU do Zabbix *server*, disponibilidades dos *hosts*, problemas por gravidade, informação do sistema entre outros.

Figura 16: *Dashboard* principal



Fonte: Elaborado pelo autor.

8.3.16 AUDITORIA

No menu relatório são apresentadas várias seções que contêm uma variedade de relatórios predefinidos e personalizáveis pelo usuário, focados em exibir uma visão geral de parâmetros como informações do sistema, *triggers* e dados coletados.

O submenu auditoria que está dentro do menu relatórios, exibe registros das alterações feitas no *front-end*, abaixo descrição das colunas:

• Hora: Carimbo de data e hora do registro de auditoria.

• Usuário: Usuário que realizou a atividade.

• IP: A partir do qual a atividade foi iniciada.

Recurso: Tipo do recurso afetado (*host*, grupo de *hosts*, etc.).

• Ação: Tipo de atividade: *Login, Logout*, Adicionado, Atualizado, Excluído, Ativado ou Desativado.

• ID: ID do recurso afetado. Ao clicar no *hiperlink* resultará na filtragem de registros de log de auditoria por essa ID de recurso.

• ID do conjunto de registros: ID compartilhado para todos os registros de log de auditoria criados como resultado da mesma operação de *front-end.*

Detalhes: Descrição do recurso e informações detalhadas sobre a atividade realizada.

A ferramenta permite a filtragem por usuário, ações, recursos, ID e ID do conjunto de registros.

A Figura 17 exibe os detalhes sobre tentativa de acesso do usuário Admin.

Figura 17: Log de Auditoria

Hora	Usuário	IP	Recurso	ID	Ação	Recordset ID	Detalhes
14-06-2023 11:54:55	Admin	10.61.43.31	Usuário	1	Login	clivu2qg80000xd2tctcztwh6	
14-06-2023 11:54:55	Admin	10.61.43.31	Usuário	1	Atualizar	clivu2qg80000xd2tctcztwh6	Descrição: Admin user.attempt_failed: 2 => 0
14-06-2023 11:54:55	guest	10.61.43.31	Usuário	2	Failed login	clivu2qg80000xd2tctcztwh6	

Fonte: Elaborado pelo autor.

9 CONCLUSÃO

Conclui-se que a solução de monitoramento Zabbix é eficiente, pois pode-se verificar que o software é capaz de realizar o monitoramento dos dispositivos de rede, medir desempenho de *hardware* para possíveis *upgrades*, gerar alerta precisos, gerenciar acesso de grupos de usuários e usuários, integrar os usuários a diretórios corporativos, organizar os dispositivos por grupos por meio de etiquetas e grupos de *hosts*, usar *templates* nativos para facilitação do gerenciamento dos itens monitorados, notificar os usuários sobre um incidente, executar comandos de emergência de forma proativa a um incidente, criar *dashboards* personalizados e auditar as alterações realizada pelos usuários no *front-end*, isso tudo auxilia para o funcionamento e gestão da infraestrutura de tecnologia da informação das organizações.

REFERÊNCIAS

Forbes. **Amazon Web Services: The Complete Story**. Junho, 2019. Disponível em: <https://www.forbes.com/sites/janakirammsv/2019/06/18/amazon-web-services-the-complete-story/?sh=3f6f49dc4a20>

LIMA, Jassen dos Reis. **Monitoramento de Redes com Zabbix**: monitore a saúde dos servidores e equipamentos de rede. Rio de Janeiro: Brasport, 2014. 8p.

ZABBIX. **Ações**. Disponível em <https://www.Zabbix.com/documentation/6.0/pt/manual/web_interface/frontend_sections/configuration/actions?hl=A%C3%A7%C3%B5es%2Ca%C3%A7%C3%B5es>. Acesso em: 06 maio 2023

ZABBIX. **Ações**. Disponível em <https://www.Zabbix.com/documentation/6.0/pt/manual/config/notifications/action?hl=A%C3%A7%C3%B5es> . Acesso em: 07 maio 2023

ZABBIX. **Agente**. Disponível em <https://www.Zabbix.com/documentation/current/pt/manual/concepts/agent>. Acesso em: 05 maio 2023

ZABBIX. **Auditoria**. Disponível em <https://www.Zabbix.com/documentation/6.0/pt/manual/web_interface/frontend_sections/reports/audit>. Acesso em: 11 maio 2023

ZABBIX. **Comandos remotos**. Disponível em <https://www.Zabbix.com/documentation/current/pt/manual/config/notifications/action/operation/remote_command >. Acesso em: 11 maio 2023

ZABBIX. **Configurações do usuário**. Disponível em <https://www.Zabbix.com/documentation/6.4/pt/manual/web_interface/user_profile> Acesso em: 05 maio 2023

ZABBIX. **Criando um item**. Disponível em <https://www.Zabbix.com/documentation/current/pt/manual/config/items/item>. Acesso em: 11 maio 2023

ZABBIX. **Definições**. Disponível em <https://www.Zabbix.com/documentation/current/pt/manual/definitions>. Acesso em: 05 maio 2023

ZABBIX. **Funcionalidades do Zabbix**. Disponível em: <https://www.Zabbix.com/documentation/current/pt/manual/introduction/features>. Acesso em: 05 maio 2023.

ZABBIX. **Geração de evento de gatilho**. Disponível em <https://www.Zabbix.com/documentation/6.0/en/manual/config/events/trigger_events?hl=event> . Acesso em: 05 maio 2023

ZABBIX. **Hosts**. Disponível em <https://www.Zabbix.com/documentation/6.0/pt/manual/web_interface/frontend_sections/monitoring/hosts?hl=Hosts%2Chosts>. Acesso em: 05 maio 2023

ZABBIX**. Itens**. Disponível em < <https://www.Zabbix.com/documentation/6.0/pt/manual/web_interface/frontend_sections/configuration/hosts/items?hl=Itens%2Citens>. Acesso em: 05 maio 2023

ZABBIX. **Marcação**. Disponível em <https://www.Zabbix.com/documentation/6.0/pt/manual/config/tagging>. Acesso em: 11 maio 2023

ZABBIX. **Modelos**. Disponível em <https://www.Zabbix.com/documentation/current/pt/manual/config/templates>. Acesso em: 05 maio 2023

ZABBIX. **Notificações sobre eventos**. Disponível em <https://www.Zabbix.com/documentation/6.0/pt/manual/config/notifications?hl=Notifica%C3%A7%C3%B5es>. Acesso em: 05 maio 2023

ZABBIX. **Novo gatilho (trigger)**. Disponível em <https://www.Zabbix.com/documentation/6.0/pt/manual/quickstart/trigger?hl=trigger>. Acesso em: 05 maio 2023

ZABBIX. **Novo host**. Disponível em <https://www.Zabbix.com/documentation/6.4/pt/manual/quickstart/host?hl=host%2CCriar>. Acesso em: 11 maio 2023

ZABBIX. **Novo modelo (template)**. Disponível em <https://www.Zabbix.com/documentation/6.0/pt/manual/quickstart/template?hl=template >. Acesso em: 05 maio 2023

ZABBIX. **O que é o Zabbix**. Disponível em: <https://www.Zabbix.com/documentation/current/pt/manual/introduction/about > . Acesso em: 05 maio 2023.

ZABBIX. **Proxy**. Disponível em <https://www.Zabbix.com/documentation/6.4/pt/manual/concepts/proxy>. Acesso em: 05 maio 2023

ZABBIX. **Registro automático de agente ativo**. Disponível em <https://www.Zabbix.com/documentation/6.0/en/manual/discovery/auto_registration?hl=autoregistration> . Acesso em: 11 maio 2023

ZABBIX. **Servidor**. Disponível em <https://www.Zabbix.com/documentation/current/pt/manual/concepts/server>. Acesso em: 05 maio 2023

ZABBIX. **Sobre a Zabbix LLC**. Disponível em: <https://www.Zabbix.com/br/about> . Acesso em: 05 maio 2023.

ZABBIX. **Tipos de mídia**. Disponível em <https://www.Zabbix.com/documentation/6.0/pt/manual/config/notifications/media?hl=M%C3%ADdias> . Acesso em: 05 maio 2023

ZABBIX. **Usuários e grupos de usuários**. Disponível em <https://www.Zabbix.com/documentation/6.4/pt/manual/config/users_and_usergroups?hl=Usu%C3%A1rios%2Cusu%C3%A1rios>. Acesso em: 05 maio 2023

ZDNet. **Hostinger Web Hosting Suffers Security Breach**. Agosto, 2019.Disponível em: <https://www.zdnet.com/article/hostinger-web-hosting-suffers-security-breach >