Gerenciamento de falha em redes utilizando boas práticas de ITIL e com o auxílio da ferramenta Zabbix para monitorar dispositivos ativos na rede de uma empresa na região de Criciúma

Henrique Lucas Roque[1] ,Me.Ricardo Alexandre Vargas Barbosa[2]

Resumo: Este estudo apresenta a aplicação das boas práticas do ITIL em conjunto com a ferramenta Zabbix para o monitoramento de dispositivos em rede. O objetivo é demonstrar como a integração dessas tecnologias pode melhorar a gestão de falhas em uma infraestrutura de TI, reduzindo o tempo de resposta e aumentando a eficiência dos serviços. A implementação foi realizada em uma empresa da região de Criciúma, com foco no monitoramento proativo e na correção de falhas.

Palavras-chave: ITIL; Zabbix; Gerenciamento de Redes; Monitoramento de Falhas; SNMP.

ABSTRACT: This study presents the application of ITIL good practices in conjunction with the Zabbix tool for monitoring network devices. The objective is to demonstrate how the integration of these technologies can improve failure management in an IT infrastructure, reducing response time and increasing service efficiency. The implementation was carried out in a company in the Criciúma region, with a focus on proactive monitoring and fault correction.

Keywords: ITIL; Zabbix; Network Management; Fault Monitoring; SNMP.

1 Introdução

Nos últimos anos, a necessidade de gerenciar grandes massas de informações se tornou cada vez mais necessária para o controle de pequenas empresas. Atualmente é visível o desenvolvimento dos meios de comunicação, buscando sempre melhores resultados e tecnologias. Este processo exige dos canais de comunicação a utilização máxima de sua capacidade, sempre com novos serviços e aplicabilidades em áreas nunca imaginadas. Com o surgimento da Internet, rede mundial de computadores, conseguiu-se níveis de comunicação eficiente, com recursos e meios que tornam o cotidiano mais simples e eficiente.

(STANGE, 2008).

Com o crescente número de equipamentos e tecnologias utilizados nas redes, somado à diversidade de problemas que podem surgir e à complexidade do diagnóstico, o processo de resolução torna-se cada vez mais desafiador e essencial. Assim, as redes são controladas usualmente por técnicos especialistas, que são encarregados de manter a disponibilidade e a qualidade dos seus serviços, efetuando o gerenciamento das mesmas (Melchiors, 1999).

Tendo em vista a melhora da eficiencia no diagnostico, com objetivo alertar de forma prévia aos gerentes de rede uma futura situação crítica na rede surge a proposta de implantação de um sistema capaz de auxiliar a corrigir, preventivamente, problemas que venham afetar o serviço de rede de uma corporação (Silva, 2011).

A fim de auxiliar no gerenciamento das falhas ocorridas na rede, sistemas de registro de problemas têm sido utilizados. Tais sistemas auxiliam os gerentes no monitoramento dos problemas correntes, mantendo um registro do ciclo de vida do problema e armazenando, com isso, a memória histórica das falhas de uma rede (Melchiors, 1999).

Para planejar o crescimento das redes estruturadas, realizar o monitoramento e garantir alta disponibilidade dos recursos, torna-se indispensável o gerenciamento eficiente das redes de computadores.Com o aumento significativo dessas redes, fica cada vez mais difícil o gerenciamento realizado somente por esforços humanos, então a adoção de ferramentas automatizadas faz-se necessária(Benicio, 2015).

As métodos relacionados ao Gerenciamento de Serviços de TI, que visam alinhar de forma dinâmica a área de TI com os objetivos do negócio, foram substancialmente fortalecidas com o estabelecimento da ITIL, um conjunto consolidado de melhores práticas para o Gerenciamento de Serviços de TI. Tal padrão elevou esses métodos a uma nova ordem de grandeza em termos de qualidade, segurança e confiabilidade de processos, situação comprovada pela maior parte das organizações usuárias de TI que as adotaram que é uma biblioteca de práticas voltadas para a aréa de tecnologia da informação (TI)(Magalhães; Pinheiro, 2007).

Baseando-se no conceito em que as redes apresentam falhas de conexão entre computadores, esse trabalho visa utilizar boas práticas de Information Technology Infrastructure Library (ITIL) para auxiliar o departamento de Tecnologia da Informação (TI), as funções da ferramenta Zabbix para monitorar os dispositivos conectados à rede,

tendo condições de controlar e monitorar em tempo real os dispositivos, com isso facilitará e diminuirá o tempo de reparo de equipamentos conectados à rede,e contribuir significativamente com a administração da Tecnologia da Informação (TI).

2 Gerenciamento de Rede

2.1 Introdução

O gerenciamento de redes é uma atividade essencial para melhorar o funcionamento correto e eficiente de uma infraestrutura. Para se realizar tais tarefas gerenciais, o uso de software específico (aqui chamados de ferramentas) tornou-se uma constante, dado o notório aumento do número de dispositivos a serem gerenciados, o que impede um tratamento individualizado de cada um, bem como dado à necessidade de procedimentos automatizados de configuração, monitoração, reportes, entre outros (Black, 2008)

Gerenciar uma rede tem se tornado uma tarefa complexa. Os gerentes de rede têm se preocupado cada vez mais em realizar um trabalho conciso, de forma a fornecer maior grau de confiabilidade para seus usuários. Dessa forma, estes profissionais precisam aprender a lidar com um crescente número de dispositivos, recursos e ferramentas disponíveis para este fim. Essa necessidade de aprendizado se justifica, também, pelo fato de que uma administração falha de uma rede pode provocar um grande impacto no funcionamento de redes corporativas de todos portes, já que a interrupção de seu funcionamento pode causar atraso ou não recebimento de dados importantes.(Leonhardt, 2005).

O gerenciamento de redes tornou-se necessário no cotidiano, facilitando a organização dos fluxos diários de atividades, seja de forma manual ou com o auxílio de sistemas automatizados. Nesse contexto, a administração dos ativos de rede ganhou importância, com foco no monitoramento de sistemas, serviços, aplicações e recursos. Sem uma gestão adequada, esses elementos podem gerar diversos problemas em uma rede de computadores.

As atividades principais do gerenciamento de redes envolvem a detecção e correção de falhas de forma rápida, além da implementação de procedimentos para prever problemas futuros. Por meio dessas ações, é possível evitar o colapso da rede, como a reconfiguração de rotas ou a substituição de roteadores por modelos mais adequados, com base na monitoração de linhas com tráfego crescente ou roteadores que estejam sobrecarregados (Leonhardt, 2005).

Gerência de rede para controlar e monitorar as operações de rede conforme os requisitos dos usuários, inclui a inicialização, monitoração e modificações tanto nos elementos de hardware quanto de software(Ferreira, 2013).

2.2 Monitoramento de Falhas

Falhas em redes são eventos não planejados que interrompem ou degradam a operação normal de sistemas de comunicação. Essas falhas podem incluir problemas de hardware, como placas de rede defeituosas; erros de configuração, como regras de firewall incorretas; e até ameaças de segurança, como ataques de negação de serviço (DDoS). Em geral, falhas de rede impactam a disponibilidade, a integridade ou a confidencialidade dos dados.

Neste contexto, as falhas monitoradas estarão relacionadas a serviços específicos que possam representar ameaças maliciosas aos dispositivos. A plataforma Zabbix será utilizada para monitoramento, com a criação de triggers configuradas para detectar serviços que possam comprometer o bom funcionamento dos dispositivos.

Na identificação do problema a verificação do número de falhas e das causas é muito importante e essencial, na medida em que se torna necessário priorizar as mais importantes para inicializar a correção das falhas. Depois se devem isolar as causas do problema, que podem influenciar na falta de conexão do restante da rede, e finalmente devesse buscar a correção da falha, pois a mesma pode gerar prejuízo, devido à indisponibilidadeda rede(Ferreira, 2013)

2.3 ITIL e Segurança

A segurança da informação dentro do contexto do ITIL é um aspecto crucial que merece atenção especial. A ITIL v4, introduziu práticas que ajudam as organizações a gerenciar riscos de segurança de forma mais eficaz. O gerenciamento de riscos é uma parte essencial do ciclo de vida do serviço, permitindo que as empresas identifiquem, analisem e mitiguem riscos de segurança que possam impactar a continuidade dos serviços(Sakamoto; Abe; Lima, 2021).

O ITIL enfatiza a importância do gerenciamento de segurança da informação como uma prática contínua, com processos que abrangem a identificação de ativos críticos, avaliação de riscos e resposta a incidentes. O módulo de gerenciamento de segurança da informação do ITIL fornece uma estrutura para proteger a confidencialidade, integridade e disponibilidade dos dados, refletindo a crescente importância da

segurança em um ambiente corporativo cada vez mais conectado.

Além disso, a norma ISO/IEC 27001 é frequentemente alinhada às práticas do ITIL para assegurar um gerenciamento eficaz da segurança da informação. A implementação dessas normas oferece uma base sólida para a proteção dos ativos de informação e a mitigação de riscos associados. A integração entre a segurança da informação e as práticas de ITIL cria um ciclo contínuo de melhoria, onde os incidentes de segurança são gerenciados e analisados para evitar recorrências(Stallings; Case, 2016).

2.4 Ferramenta Zabbix

O Zabbix é um software que monitora vários parâmetros da rede, dos servidores e da saúde dos serviços. Utiliza-se de um mecanismo flexível de notificação que permite configurar alertas por email para praticamente qualquer evento. As notificações permitem que se reaja rapidamente à problemas no ambiente. O Zabbix oferece excelentes recursos de relatórios e visualização de dados armazenados. Isso faz com que o Zabbix seja a ferramenta ideal para planejamento de capacidade(Zabbix, 2024).

Essa ferramenta oferece funcionalidades avançadas, como monitoramento em tempo real, alertas proativos e relatórios detalhados, que são essenciais para a detecção precoce e a resolução rápida de problemas de rede.

Zabbix é um software que utiliza o tipo servidor agente de funcionamento, permitindo mais de um servidor rodando ao mesmo tempo redundante, por tanto recolhendo os dados gerados por seus agentes rodando nos mais diversos clientes.

A arquitetura do Zabbix é distribuída e isso implica que não é possível ter um gerente central para gerenciar todas informações e dados dos demais gerentes e clientes. Estes dados são armazenados em bancos de dados relacionais MySQL, PostgreSQL ou Oracle e o software pode rodar em todas distribuições Linux/Unix. Seus agentes estão disponíveis para sistemas operacionais Linux, Unix (AIX, HP-UX), MacOS X, Solaris, FreeBSD, Netware, Windows e dispositivos rodando SNMP v1, v2 e v3(Black, 2008).

2.5 Monitoramento com Zabbix Agent

O monitoramento de redes com Zabbix é funcional a partir do protocolo SNMP e através do agente Zabbix. Em todos os casos, esses

protocolos servem para capturar e mostrar as informações em tempo real ao gestor da rede em acompanhamento(PAULO HENRIQUE OLIVEIRA, 2022).

Além dos alertas, a prática do monitoramento de rede propõe uma facilidade em centralizar os dados coletados, transformando estes em gráficos simples e objetivos para que o administrador responsável pelo sistema ou rede possa acompanhar o desempenho e os resultados da sua aplicação(ANDRADES, 2021).

O Zabbix é usado para monitorar dispositivos ativos em uma rede, como servidores, switches, roteadores e outros dispositivos de rede. Ele permite configurar itens de monitoramento, criar gatilhos para alertas evisualizar dados em tempo real e históricos em painéis personalizados.

Os principais módulos de monitoramento do Zabbix são:

- Zabbix server
- Zabbix proxy
- Zabbix agent

2.6 Monitoramento com Zabbix SNMP

O protocolo SNMP é utilizado para gerenciamento de redes. Ele permite que dispositivos de rede comuniquem informações de gerenciamento para um sistema de monitoramento centralizado, sendo utilizados para efetuar essa comunicação NMS(Network management software).

O gerenciamento da rede através do SNMP permite o acompanhamento simples e fácil do estado, em tempo real, da rede, podendo ser utilizado para gerenciar diferentes tipos de sistemas(Dias; Jr, 2001).

O protocolo SNMP é utilizado para obtenção de estatísticas de equipamentos conectados a determinados computadores operando como servidores, equipamentos estes operando em uma rede baseada nos protocolos do modelo de redes TCP/IP(Esteves; Jr, 2013).

Os dados são obtidos via requisições de um dado gerente a um ou mais agentes, para isto utilizando-se o protocolo de transporte UDP User Datagram Protocol, responsável pelas atividades de envio e recebimento de mensagens através de uma rede qualquer(Esteves; Jr, 2013).

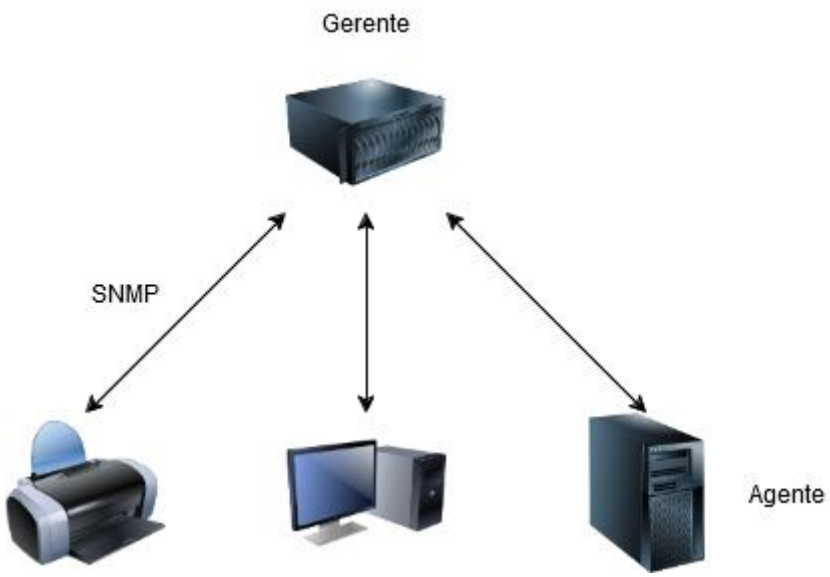
Este gerenciamento é conhecido como modelo de gerenciamento SNMP, ou simplesmente, gerenciamento SNMP.

O protocolo SNMP é composto por três componentes:

1. Agentes SNMP: Esses são softwares que residem nos dispositivos de rede e coletam informações sobre o dispositivo, como status da CPU,tráfego de rede, uso de memória, entre outros.
2. Gerentes SNMP: Estes são os sistemas de gerenciamento de rede, que emitem solicitações de informações para os agentes SNMP nos dispositivos de rede. Os gerentes SNMP podem ser softwares dedicados ou sistemas integrados em outras ferramentas de gerenciamentode rede.
3. MIB (Management Information Base): A MIB é uma base de informações hierárquica que define os objetos gerenciáveis disponíveis nos dispositivos de rede. Cada objeto na MIB tem um identificador único chamado de OID (Object Identifier).

Conforme Figura 1 Ilustrada abaixo,O funcionamento do SNMP é baseado em dois dispositivos o agente e o gerente. Cada máquina gerenciada é vista como um conjunto de variáveis que representam informações referentes ao seu estado atual, estas informações ficam disponíveis ao gerente através de consulta e podem ser alteradas por ele. Cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB.(Dias; Jr, 2001).

Figura 1: Protoloco SNMP



Fonte:Elaborado pelo autor(2024).

Desde sua criação, a segurança tem sido considerada a maior vulnerabilidade do SNMP. Originalmente projetado para facilitar o gerenciamento de dispositivos em redes, o SNMP nas versões 1 e 2 priorizava simplicidade e funcionalidade, mas carecia de mecanismos robustos de proteção, o que o tornava vulnerável a ataques como interceptação de dados, acessos não autorizados e manipulação maliciosa de informações. Embora versões mais recentes, como o SNMPv3, tenham introduzido melhorias significativas em segurança, incluindo autenticação e criptografia, a adoção restrita dessas versões mais seguras ainda representa um desafio para a proteção das redes que utilizam o protocolo.

A autenticação SNMP nas versões 1 e 2 equivale a nada mais do que uma identificação(string de comunidade), enviada em texto não criptografado entre o gerente e o agente.

2.5.1 ITIL e Gerenciamento de Serviços de TI

O ITIL é uma estrutura de melhores práticas para a gestão de serviços de TI que visa alinhar a TI aos objetivos organizacionais, garantindo qualidade e consistência na prestação de serviços. A versão 4 do ITIL, lançada em 2019, introduziu novos conceitos e ampliou o escopo para abranger práticas de gerenciamento de incidentes, problemas, mudanças, ativos, e monitoramento de eventos, entre outras. Ao oferecer um ciclo de vida completo para os serviços de TI, o ITIL permite que empresas integrem seus processos de TI de forma coesa, promovendo a comunicação e o compartilhamento de informações entre diferentes etores (Zendesk, 2023).

- **Gerenciamento de Incidentes:** Focado em restaurar os serviços de TI para o funcionamento normal o mais rápido possível após uma interrupção, o gerenciamento de incidentes é essencial para reduzir o impacto de falhas. O processo é estruturado para que incidentes sejam identificados, classificados e resolvidos conforme sua prioridade, com o objetivo de minimizar os prejuízos operacionais e financeiros.

- **Gerenciamento de Problemas:** Diferente dos incidentes, o gerenciamento de problemas se concentra na identificação e eliminação das causas raiz das falhas. Problemas recorrentes ou

críticos são documentados e analisados, permitindo que a equipe de TI implemente soluções permanentes e evite a reincidência de incidentes.

Essas práticas, quando implementadas em conjunto com o Zabbix, possibilitam uma abordagem proativa ao gerenciamento de redes, trans- formando o monitoramento reativo em uma prática preditiva e preventiva.

Esta integração permite uma abordagem mais proativa na ges tão de falhas, alinhando os processos de monitoramento com os objetivos estratégicos da empresa, sendo necessário ferramentas para monitorar o cotidiano, é necessário possuir um método uma maneira de efetuar essa organização de uma TI.

Com foco nos frameworks de ITIL para o gerenciamento de segurança e gerenciamento de falhas em uma rede de computadores, a proposta é aplicar esses princípios junto ao Zabbix para melhorar a visualização e controle dessa rede de dispositivos conectados.

Integrar o Zabbix com ITIL envolve configurar o Zabbix para monitorar a infraestrutura de TI e detectar eventos que possam se transformarem incidentes conforme as práticas do ITIL. A configuração de triggers no Zabbix permite a detecção de problemas específicos, enquanto alertas e notificações automáticas garantem que os responsáveis sejam informadosimediatamente.

Para automatizar o gerenciamento de incidentes, o Zabbix podeser integrado com sistemas ITSM, como ServiceNow ou Jira Service Management, usando APIs ou webhooks para criar tickets automaticamente. Isso possibilita a categorização e priorização dos incidentes com base na severidade, alinhando o monitoramento proativo do Zabbix com o fluxo de trabalho de gerenciamento de serviços de TI segundo o ITIL.

3 Metodologia

3.1 Experimento e Ambiente de Testes

O ambiente de testes consistiu em uma configuração que simula a infraestrutura de uma empresa de médio porte, com diversos dispositivos de rede conectados, incluindo switches gerenciáveis, roteadores e servidores. A implementação do Zabbix foi realizada em um servidor dedicado, configurado para monitorar todos os dispositivos conectados por meio do protocolo SNMP.

Para testar a eficiência do sistema, foram configurados alertas

que notificam a equipe de TI sobre situações críticas, como perda de conectividade e alta utilização de recursos. O ambiente de testes incluiu:

- **Hardware:** Computador com 8GB de RAM, processador de 1,4GHz e disco de 500GB, além de um switch gerenciável de 10 portas gigabit.
- **Software:** Zabbix 7.0 LTS, Grafana 6,4 e instalado em um servidor com sistema operacional Ubuntu 24.04 LTS.
- **Dispositivos Monitorados:** Servidores, firewall, Computadores, roteadores e switches configurados para serem monitorados pelo Zabbix, com agentes ou SMNP aplicados.

3.2 Coleta de Dados e Configuração do Monitoramento

O monitoramento foi configurado para coletar dados continuamente, com foco em indicadores de desempenho como uso de CPU, memória e largura de banda. Gatilhos foram configurados para que, ao detectar valores críticos, o Zabbix automaticamente envie um alerta para o responsável. Os testes incluíram:

- **Monitoramento de Carga e Disponibilidade:** Configuração de alertas para identificar picos de utilização e quedas de serviço.
- **Resolução de Incidentes:** Configuração de respostas automáticas para reiniciar serviços e realizar diagnósticos em tempo real.

3.3 Testes de Performance e Validação das Práticas ITIL V4

Os testes foram realizados para verificar a eficácia do sistema em detectar falhas e notificar a equipe de TI. Incidentes simulados incluíram sobrecarga de CPU e falhas de rede, permitindo avaliar o tempo de resposta do Zabbix e a precisão dos alertas. O desempenho foi medido com base na rapidez de notificação e na capacidade do sistema de restaurar a operação normal.

4 Resultados e Discussão

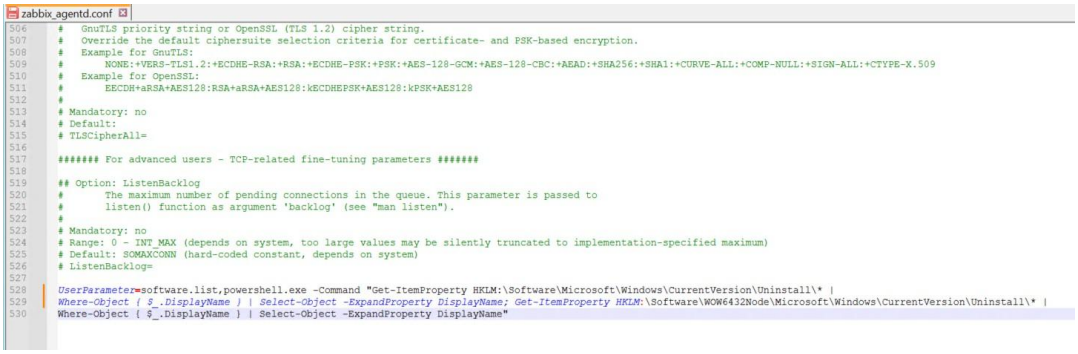
Para aprimorar o controle sobre os recursos de TI, foram desenvolvidas funções e scripts personalizados, tanto no Zabbix Agent quanto no próprio Zabbix Server, focados no monitoramento detalhado de aplicativos instalados e portas de rede utilizadas nos servidores e estações de trabalho.

Essas funcionalidades permitem identificar e listar automaticamente todos os softwares em uso nos dispositivos monitorados, registrando suas versões e status de licença. Dessa forma, a equipe de TI consegue acompanhar a conformidade com as políticas de software,

identificando instalações não autorizadas ou desatualizadas, sem a necessidade de verificação manual em cada máquina.

Conforme ilustrado na Figura 2, o script gerado para obter os softwares instalados em uma máquina na rede, sendo aplicado no arquivo de configuração do zabbix aget(zabbix-agent.conf).

Figura 2: Configuração Agent

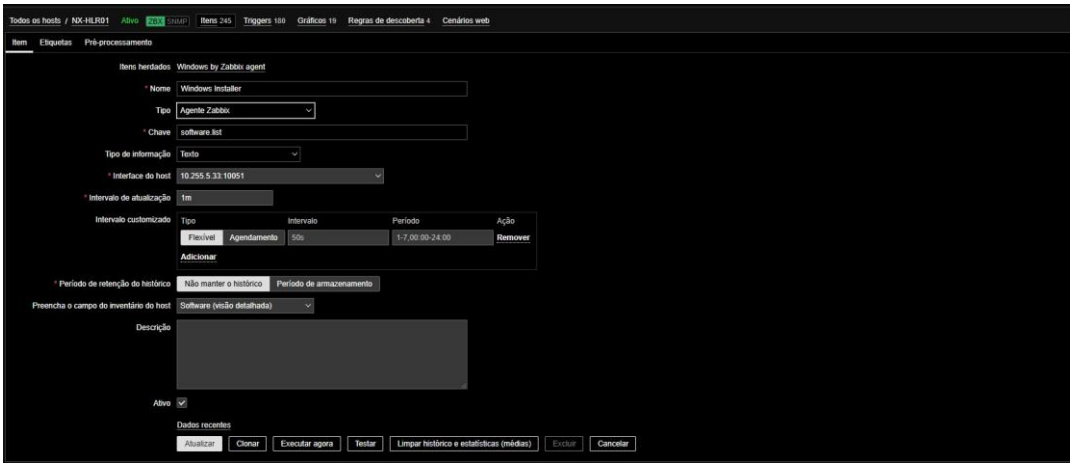


Fonte:Elaborado pelo autor(2024).

O scritp é formado pelas linhas 528 a 530, sendo priorizadas para obter o nome e versão dos aplicativos que estão instalados na base 32bits e 64bits do computador.

Conforme ilustrado na Figura 3, foi realizada a configuração do servidor Zabbix Server para interpretar o script. Para isso, foi necessário utilizar a chave “software.list” para consultar os aplicativos instalados.

Figura 3: Aplicativos Instalados



Fonte:Elaborado pelo autor(2024).

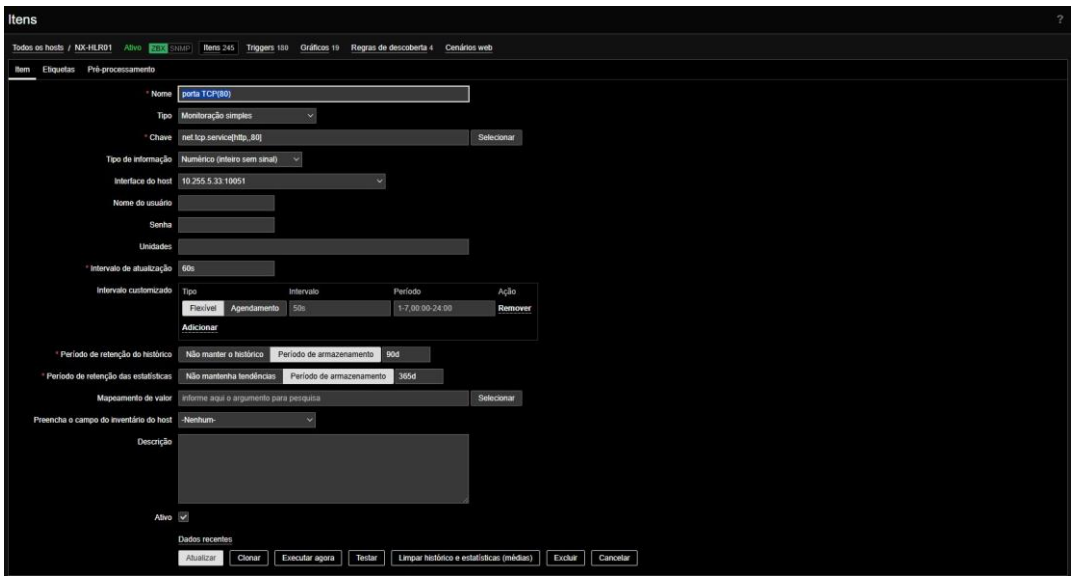
4.1.1 Monitoramento de portas

O monitoramento das portas abertas e em uso permite rastrear possíveis vulnerabilidades e identificar conexões não autorizadas, como

a ativação indevida de portas críticas, que podem representar riscos à segurança, ou o bloqueio acidental de portas essenciais para serviços, como a porta 3389 utilizada para acesso remoto. Essas análises permitem ajustes imediatos e evitam interrupções em serviços críticos, garantindo uma infraestrutura de TI mais segura e eficiente.

Conforme ilustrado na Figura 4, observer que a configuração é feita interamente no zabbix, pois ele nos permite adicionar novas regras de monitoramento especifico como monitoramento das portas TCP e UDP, gerando assim um foco em determinadas portas a serem monitoradas.

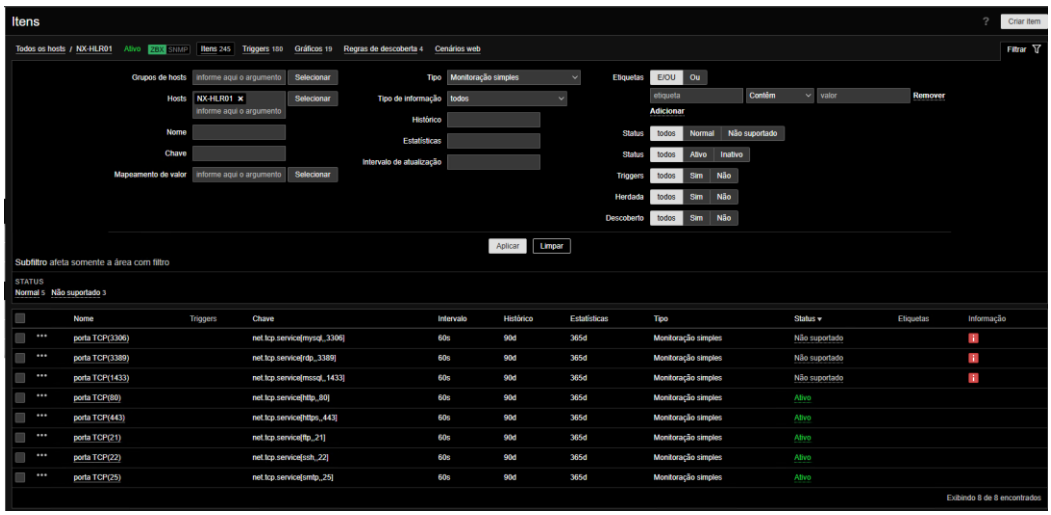
Figura 4: Configuração Portas



Fonte:Elaborado pelo autor(2024).

Seguindo abaixo a Figura 5, são ilustradas algumas portas que estão sendo monitoradas pelo agent Zabbix.

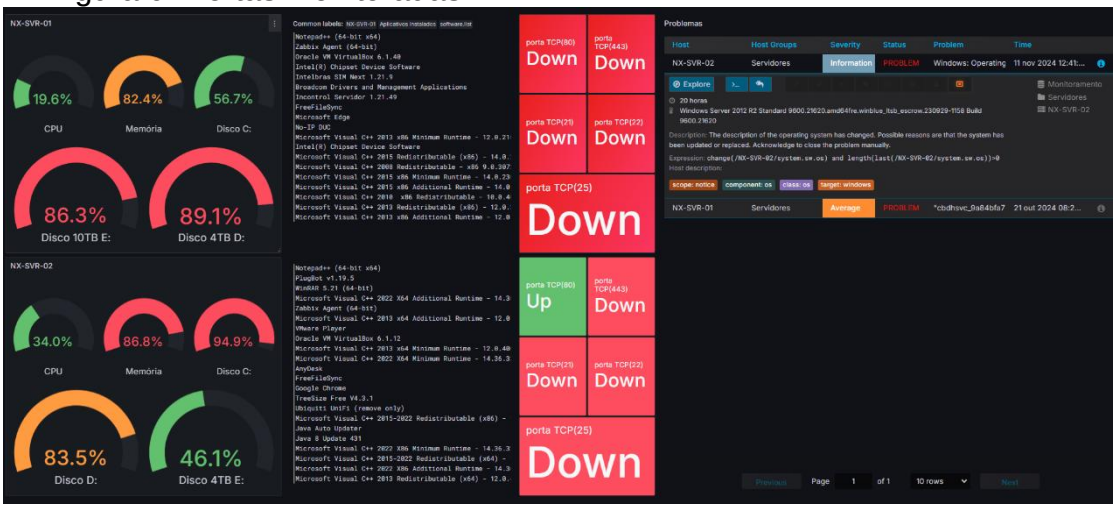
Figura 5: Portas monitoradas



Fonte:Elaborado pelo autor(2024).

Neste caso, foi desenvolvida uma interface diretamente integrada ao Grafana para aprimorar a visualização e o monitoramento das portas abertas para uso, permitindo verificar se os serviços estão ativos ou inativos, conforme ilustrado na Figura 6.

Figura 6: Portas monitoradas



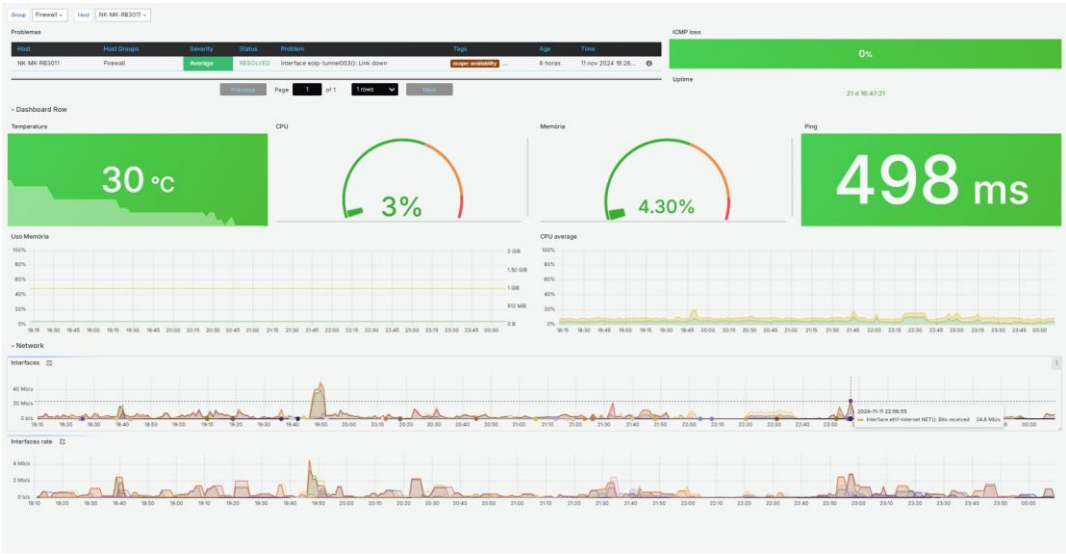
Fonte:Elaborado pelo autor(2024).

4.1.2 Monitoramento de SMNP

O monitoramento por meio do protocolo SNMP v2 está sendo utilizado para acompanhar o uso de banda e o consumo de processamento do firewall e do switch da rede de computadores. As principais interfaces de rede são monitoradas em tempo real, tornando a interface mais amigável ede fácil configuração.

A interface gráfica foi desenvolvida com base nos conceitos do ITIL V4, proporcionando maior interação com o Zabbix, como demonstrado na Figura 7. Para uma visualização aprimorada das conexões, incluindo o uso de banda e as interrupções nas interfaces conectadas, sendo utilizado a ferramenta Grafana como mediador.

Figura 7: Interface Grafana



Fonte:Elaborado pelo autor(2024).

4.1 Implementação de ITIL V4

A implementação das práticas ITIL junto ao monitoramento pelo Zabbix resultou em uma melhoria significativa na eficiência do gerenciamento de rede, especialmente em termos de tempo de resposta e mitigação de incidentes. Durante o período de testes, os principais resultados observados incluem:

1. **Redução no Tempo de Resolução de Incidentes:** Com os alertas automáticos configurados no Zabbix, a equipe de TI foi notificada imediatamente sobre incidentes como a sobrecarga de CPU e falhas de conectividade, Com isso conseguimos identificar que um computador da rede estava com falhas pois estava tendo queda de energia toda a noite e com isso ocorreram falhas de serviços do windows. Essa notificação em tempo real reduziu o tempo de resposta de incidentes, quando comparado ao processo tradicional de monitoramentomanual.
2. **Melhoria na Visibilidade e Controle de Ativos:** A implementação do Zabbix proporcionou uma visão centralizada e detalhada dos dispositivos conectados à rede. Os gráficos gerados em tempo real permitiram monitorar picos de uso de recursos, como CPU e tráfego de rede, possibilitando à equipe identificar rapidamente os dispositivos mais sobrecarregados e aplicar medidas preventivas, como a redistribuição de tarefas entre servidores. Além disso, o Zabbix facilitou a verificação de softwares instalados nos computadores, sem a necessidade de acesso físico ou de consulta

aos usuários, permitindo também a detecção de aplicativos não autorizados.

3. **Eficiência no Diagnóstico e na Identificação de Causas Raiz:** Combinando as práticas de gerenciamento de incidentes e problemas do ITIL com o uso do Zabbix, foi possivel identificar padrões de falhas recorrentes e construir um histórico de problemas. Essa análise permitiu uma abordagem mais proativa na resolução de problemas, como a verificação do uso de recurso de determinado serviço que estava excedendo o consumo do computador fazendo com que travasse, sendo resolvido o mais rápido possivel antes que a falha recorrente não impactasse a operação da rede.

4. **Maior Confiabilidade na Infraestrutura de TI**: O monitoramento contínuo aumentou a confiabilidade e a disponibilidade dos serviços de TI. Tendo como exempro pratico a identificação de possíveis falhas, como interrupções inesperadas em serviços essenciais como bancos de dados SQL Server, antes que se tornem críticas. Isso resultou em uma melhora na qualidade dos serviços oferecidos e consequentemente, na satisfação dos usuários.

4.2 Limitações e Implicações Práticas

Apesar dos resultados positivos, algumas limitações foram observadas. Em redes maiores, o protocolo SNMP pode apresentar vulnerabilidades de segurança, especialmente nas versões anteriores ao SNMPv3. Isso pode limitar a aplicabilidade da solução em redes com alto grau de confidencialidade e requisitos de segurança. Além disso, a implementação das práticas ITIL exige uma curva de aprendizado, com treinamento da equipepara adaptação aos novos processos de trabalho.

As implicações práticas deste estudo são claras: a combinação de ITIL e Zabbix representa uma solução eficaz e econômica para o gerenciamento de redes de pequeno e médio porte. Pequenas e médias emspresas podem beneficiar-se da automação proporcionada pelo Zabbix, ao mesmo tempo em que adotam um processo de gestão estruturado com as práticas ITIL. Isso permite que essas empresas obtenham uma infraestrutura de TI mais robusta, com redução no tempo de inatividade e melhora naqualidade dos serviços.

5 Conclusão

Este estudo demonstrou que a integração das práticas ITIL com o Zabbix é uma estratégia viável e eficaz para o gerenciamento de

falhas em redes corporativas. Os testes realizados mostraram que a combinação dessas ferramentas pode proporcionar uma redução significativa no tempo de resposta a incidentes e uma maior confiabilidade da infraestrutura de TI. A abordagem integrada, que inclui monitoramento contínuo e práticas estruturadas de resposta a incidentes, provou ser eficaz na detecção, análise e resolução de problemas de rede.

A principal contribuição deste estudo é a proposta de uma solução prática e acessível para pequenas e médias empresas que desejam otimizar o gerenciamento de redes com custos reduzidos. A aplicação conjunta das práticas ITIL e do Zabbix fornece um modelo de monitoramento e gerenciamento de falhas que pode ser implementado sem a necessidade de grandes investimentos. Este modelo oferece uma base para que empresas de menor porte obtenham uma infraestrutura de TI mais eficiente e segura, aumentando a qualidade dos serviços e a satisfação dos usuários.

6 Trabalhos Futuros

Para aprofundar o entendimento sobre a eficácia desta integração, recomenda-se que futuros estudos explorem o uso de inteligência artificial para aprimorar a detecção e previsão de falhas, integrando o Zabbix com algoritmos de machine learning. Essas tecnologias poderiam analisar os dados históricos de monitoramento para prever falhas futuras, possibilitando uma abordagem ainda mais proativa e preventiva ao gerenciamento de redes. Além disso, a ampliação deste estudo para ambientes de rede híbrida, que incluam tanto redes locais quanto componentes em nuvem, poderá oferecer insights adicionais sobre a flexibilidade e escalabilidade da solução proposta.

REFERÊNCIAS

ANDRADES, L. B. D. Rede corporativa. [S.l.], 2024.

BENICIO, W. E. P. Monitoramento e gerenciamento de redes utilizando Zabbix. Trabalho apresentado ao Curso de Análise e Desenvolvimento de Sistemas do Instituto Federal como requisito para obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas, 2024.

BLACK, T. L. Comparação de ferramentas de gerenciamento de redes. [S.l.], 2024.

COMER, Douglas. Interligação de Redes com TCP/IP: Princípios, Protocolos e Arquitetura. 1. ed. [S.l.]: Elsevier Brasil, 2016. v. 1.

DIAS, B. Z.; JR, N. A. Protocolo de gerenciamento SNMP. Nota Técnica CBPF-NT-006/01, 2001.

ESCOLA LINUX. Monitoramento de redes com Zabbix: o que é e como funciona? 2022. Acesso em: 12 jun. 2024. Disponível em: https://nova.escolalinux.com.br/blog/monitoramento-de-redes-com-zabbix-o-que-e-e-como-funciona.

ESTEVES, A. M. B.; JR, N. A. O protocolo SNMP. Notas Técnicas, v. 3, n. 1, 2001.

EUAX. ITIL 4: confira o que mudou no framework e descubra como criar valor através de serviços de TI. [S.l.: s.n.], 2018. Acesso em: 10 jun. 2024. Disponível em: https://www.euax.com.br/2018/10/itil-o-que-e-importancia-como-implantar/.

FERREIRA, F. S. Impactos e influências do gerenciamento de redes. Universidade Presbiteriana Mackenzie, 2024.

FOROUZAN, Behrouz A.; FEGAN, Sophia Chung. Protocolo TCP/IP-3. [S.l.]: AMGH Editora, 2009.

FOROUZAN, Behrouz A.; MOSHARRAF, Firouz. Redes de computadores: uma abordagem top-down. [S.l.]: AMGH Editora, 2013.

LEMES, João Éder Ancelmo. Monitoramento em redes IPv6 com Zabbix e Raspberry Pi. Universidade Tecnológica Federal do Paraná, 2014.

LEONHARDT, M. D. Doroty: um chatterbot para treinamento de profissionais atuantes no gerenciamento de redes de computadores. [S.l.], 2024.

MAGALHÃES, I. L.; PINHEIRO, W. B. Gerenciamento de serviços de TI na prática: uma abordagem com base na ITIL: inclui ISO/IEC 20.000 e IT Flex. [S.l.]: Novatec Editora, 2007.

MELCHIORS, C. Raciocínio baseado em casos aplicado ao gerenciamento de falhas em redes de computadores. [S.l.], 2024.

SAKAMOTO, L. S.; ABE, J. M.; LIMA, L. A. de. Análise de risco do controle de mudança utilizando lógica paraconsistente anotada evidencial. Anais Aspectos de Sistemas Inteligentes Baseados em Lógicas Anotadas, p. 129, 2024.

SILVA, F. C. d. Rede neural artificial para detecção de falhas em redes locais. Universidade Tecnológica Federal do Paraná, 2024.

STALLINGS, W.; CASE, T. Redes e sistemas de comunicação de dados. [S.l.]: Elsevier Brasil, 2016.

STANGE, R. Ferramenta para gerenciamento de falhas em rede Ethernet baseada em protocolo SNMP. [S.l.], 2024.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO. Simple Network Management Protocol. 2010. Acesso em: 3 jun. 2024. Disponível em: https://www.gta.ufrj.br/grad/10_1/snmp/index.htm.

ZABBIX SIA. Documentation. [S.l.: s.n.], 2024. Acesso em: 10 jun. 2024. Disponível em: https://www.zabbix.com/documentation/3.4/pt/manual/introduction/about.