



UNIVERSIDADE ESTADUAL DO PIAUÍ
CENTRO DE TECNOLOGIA E URBANISMO
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

Carlos Matheus Ferreira de Oliveira

**Melhorias no Monitoramento de Servidores
On-Premise com Centreon: Uma Abordagem Prática
Aplicada à Prodater**

TERESINA

2025

Carlos Matheus Ferreira de Oliveira

**Melhorias no Monitoramento de Servidores
On-Premise com Centreon: Uma Abordagem Prática
Aplicada à Prodater**

Monografia de Trabalho de Conclusão de Curso apresentado na Universidade Estadual do Piauí – UESPI como parte dos requisitos para conclusão do Curso de Bacharelado em Ciência da Computação.

Orientador: Carlos Giovanni Nunes de Carvalho

TERESINA
2025

048m Oliveira, Carlos Matheus Ferreira de.

Melhorias no monitoramento de servidores on-premise com Centreon: uma abordagem prática aplicada à Prodater / Carlos Matheus Ferreira de Oliveira. - 2025.

30f.: il.

Monografia (graduação) - Curso de Bacharelado em Ciência da Computação, Universidade Estadual do Piauí, 2025.

"Orientação: Prof. Dr. Carlos Giovanni Nunes de Carvalho".

1. On-premise. 2. Centreon. 3. Servidores. 4. Monitoramento. 5. Alarmes. I. Carvalho, Carlos Giovanni Nunes de . II. Título.

CDD 004.8

Carlos Matheus Ferreira de Oliveira

Melhorias no Monitoramento de Servidores On-Premise com Centreon: Uma Abordagem Prática Aplicada à Prodater/ Carlos Matheus Ferreira de Oliveira. – Teresina – PI, Brasil, 2025.

Orientador: Carlos Giovanni Nunes de Carvalho

Monografia (Graduação) – Universidade Estadual do Piauí, 2025.

1. Embarcado. 2. GSM. 3. GPS. 3. RF 433 Mhz. I. Nome do Orientador. II. Universidade Estadual do Piauí.

Melhorias no Monitoramento de Servidores On-Premise com Centreon: Uma Abordagem Prática Aplicada à Prodater

Carlos Matheus Ferreira de Oliveira

Monografia de Trabalho de Conclusão de
Curso apresentado na Universidade Esta-
dual do Piauí – UESPI como parte dos re-
quisitos para conclusão do Curso de Bacha-
relado em Ciência da Computação.

Documento assinado digitalmente
gov.br CARLOS GIOVANNI NUNES DE CARVALHO
Data: 16/07/2025 07:47:13-0300
Verifique em <https://validar.itи.gov.br>

**Carlos Giovanni Nunes de Carvalho, Dsc.
Orientador**

Teresina, 03 de Julho de 2025
Nota da Banca Examinadora: 8,5

Banca Examinadora:

Documento assinado digitalmente
gov.br CARLOS GIOVANNI NUNES DE CARVALHO
Data: 16/07/2025 07:47:55-0300
Verifique em <https://validar.itи.gov.br>

**Carlos Giovanni Nunes de Carvalho,
Dsc.
Presidente**

Documento assinado digitalmente
gov.br JOSE DE RIBAMAR MARTINS BRINGEL FILHO
Data: 04/09/2025 09:39:26-0300
Verifique em <https://validar.itи.gov.br>

**José De Ribamar Martins Bringel Filho
Dsc.
Membro**

Documento assinado digitalmente
gov.br Reginaldo Rodrigues das Gracas
Data: 18/07/2025 18:52:21-0300
Verifique em <https://validar.itи.gov.br>

**Reginaldo Rodrigues Das Graças
Msc.
Membro**

*Este trabalho é dedicado às crianças adultas que,
quando pequenas, sonharam em se tornar cientistas.*

AGRADECIMENTOS

Agradeço à Deus pela minha vida e pela vida de todas as pessoas que fazem parte dela.

A minha mãe e meu pai por me incentivarem a cada dia a alcançar meus sonhos, paciência, amor e suporte na minha árdua caminhada até aqui.

A minha esposa Lara Raquel Vasconcelos da Silva Ferreira por sempre me apoiar e me incentivar para finalizar o curso. Te amo!

A Todos meus professores desta universidade por me orientar e me guiar durante todo o curso.

A grandes amizades que fiz durante o curso e que levarei para a vida.

A todos que direta ou indiretamente fizeram parte da minha formação.

*“A arma mais forte em dois milhões de anos
de história humana: tecnologia de comunicação.”*
(Inagaki, Riichiro; Dr. Stone, 2019)

RESUMO

Este trabalho de conclusão de curso tem como objetivo principal propor melhorias e otimizações no ambiente de servidores on-premise da empresa pública Prodater, com foco na implementação e aprimoramento de sistemas de monitoramento e alarmes utilizando a ferramenta Centreon. Considerando que a Prodater já utilizava o Centreon para monitoramento básico, a escolha por essa ferramenta foi motivada pela familiaridade, robustez e flexibilidade oferecidas. A pesquisa envolveu a instalação de um ambiente de testes local, onde foram realizadas as configurações de monitoramento e alarmes, possibilitando o aprendizado prático e a customização da solução. Posteriormente, as configurações foram aplicadas ao ambiente de produção. O referencial teórico abordou conceitos como gestão de infraestrutura de TI, ITIL v4, MTTR e os estados dos serviços monitorados. Os resultados mostraram uma melhoria significativa na detecção precoce de falhas, no tempo de resposta e na organização dos alertas. O trabalho também destacou as limitações da solução atual e apontou caminhos para futuras melhorias.

Palavras-chaves: Monitoramento, Centreon, Alarmes, Servidores, On-premise, ITIL v4, MTTR.

ABSTRACT

This final undergraduate project aims to propose improvements and optimizations to the on-premise server environment of the public company Prodater, focusing on the implementation and enhancement of monitoring and alert systems using the Centreon tool. Since Prodater already employed Centreon for basic monitoring, the decision to continue with this platform was based on its robustness, flexibility, and existing familiarity. The research included the setup of a local testing environment, where all monitoring and alert configurations were carried out, allowing practical learning and customization. These configurations were later applied to the production environment. The theoretical framework discussed concepts such as IT infrastructure management, ITIL v4, MTTR, and the service status model. The results indicated significant improvements in early failure detection, response time, and alert organization. The project also addressed current limitations and proposed directions for future enhancements.

Keywords: Monitoring, Centreon, Alerts, Servers, On-premise, ITIL v4, MTTR.

LISTA DE ILUSTRAÇÕES

Figura 1 – Instalação completa e login admin	20
Figura 2 – Notificação personalizada para envio de chamda de API quando acionado o alarme	21
Figura 3 – Configuração dos serviços via template	22
Figura 4 – Chamadas realizadas na api pelo Centreon em cada envio de notificação	24
Figura 5 – Frontend com alertas recebidos	25
Figura 6 – Descrição de alarme recebido com botão de reconhecer alerta	26
Figura 7 – Alerta reconhecido pelo usuário	26

LISTA DE QUADROS

SUMÁRIO

1	INTRODUÇÃO	13
2	REFERENCIAL TEÓRICO	15
2.1	Infraestrutura de TI On-Premise	15
2.2	Monitoramento de Sistemas de TI	15
2.3	Alarms e Notificações em Ambientes de TI	16
2.4	A Ferramenta Centreon	16
2.5	MTTR - Mean Time to Repair	16
2.6	Hosts e Serviços no Centreon	17
2.6.1	Estados de Monitoramento: OK, WARNING, CRITICAL e UNKNOWN	18
2.7	Práticas de Monitoramento Proativo	18
3	DESENVOLVIMENTO	19
3.1	Contexto da Implementação	19
3.2	Instalação Local do Centreon	19
3.3	Configuração do Sistema de Alarmes	20
3.4	Definição de Limites para os Alarmes	21
3.5	Transição para Ambiente de Produção	22
3.6	Resultados	23
4	CONCLUSÕES	28
4.1	Contribuições	28
4.2	Limitações	28
4.3	Trabalhos Futuros	29
	REFERÊNCIAS	30

1 INTRODUÇÃO

A infraestrutura de Tecnologia da Informação (TI) é um pilar essencial para o funcionamento e a continuidade operacional das organizações modernas, sejam públicas ou privadas. Entre os principais componentes dessa infraestrutura, os servidores desempenham papel central ao hospedar aplicações, armazenar dados e suportar processos críticos do negócio. Embora a computação em nuvem esteja em constante crescimento, muitos órgãos e empresas ainda mantêm seus servidores em ambientes locais — os chamados ambientes *on-premise* — por razões como segurança, controle, conformidade legal ou restrições contratuais.

Esse é o caso da Empresa de Processamento de Dados da Prefeitura de Teresina (PRODATER), que mantém uma infraestrutura de servidores *on-premise* para atender suas demandas. Apesar da robustez e do controle que esse tipo de ambiente oferece, a sua gestão eficaz apresenta desafios recorrentes, especialmente no que diz respeito à visibilidade operacional, resposta a incidentes, desempenho e continuidade dos serviços.

O monitoramento proativo de recursos de TI se destaca como uma estratégia essencial para garantir a estabilidade e a eficiência do ambiente computacional. Entretanto, mesmo com ferramentas de monitoramento como o Centreon já implantadas em determinadas instituições, como é o caso da PRODATER, muitas vezes faltam funcionalidades críticas, como a correta configuração de alarmes e notificações, que são indispensáveis para detectar e reagir rapidamente a falhas.

Diante desse contexto, identificou-se a necessidade de aprimorar o sistema de monitoramento da PRODATER por meio da implementação de um sistema eficiente de alarmes, utilizando a própria ferramenta Centreon — já adotada institucionalmente, o que facilitou a continuidade da solução. Como o ambiente produtivo da PRODATER está sob controle de uma empresa terceirizada, a aplicação prática inicial deste trabalho foi realizada em uma instalação controlada localmente. Esse ambiente permitiu maior liberdade para estudar, testar e configurar o Centreon de maneira adequada antes da transição para o ambiente de produção.

Dessa forma, o presente Trabalho de Conclusão de Curso (TCC) tem como objetivo geral analisar e demonstrar a aplicação da ferramenta Centreon para implementar um sistema eficaz de monitoramento e alarmes em um ambiente de servidor *on-premise*, avaliando seu impacto na otimização de recursos, na detecção proativa de falhas e na melhoria da gestão operacional.

Para alcançar esse objetivo geral, foram definidos os seguintes objetivos espe-

cíficos:

- Analisar os desafios e as deficiências de um ambiente de servidor *on-premise* operando sem um sistema de alarmes devidamente configurado.
- Apresentar a ferramenta Centreon, detalhando sua arquitetura, principais componentes e funcionalidades relevantes para o monitoramento de servidores e a configuração de alarmes.
- Descrever o processo de implementação e configuração do Centreon em ambiente controlado, com foco na definição de métricas e criação de alarmes e notificações.
- Avaliar os benefícios da implementação da solução, especialmente no que diz respeito à redução do tempo médio de resposta a incidentes (MTTR), à melhoria da visibilidade da infraestrutura e à transformação da abordagem reativa em proativa.

A metodologia utilizada inclui pesquisa bibliográfica sobre conceitos de infraestrutura *on-premise*, monitoramento de sistemas e práticas recomendadas para gestão de TI, bem como a realização de um estudo de caso aplicado na instalação controlada do Centreon, com posterior validação na infraestrutura da PRODATER.

A relevância deste estudo se justifica pela necessidade crescente de visibilidade operacional em ambientes de TI, especialmente em órgãos públicos que enfrentam restrições orçamentárias e operacionais. A ausência de mecanismos de monitoramento pode levar à indisponibilidade de serviços essenciais, prejuízos operacionais e comprometimento da continuidade dos negócios.

2 REFERENCIAL TEÓRICO

Este capítulo apresenta os principais conceitos, fundamentos e estudos que embasam o desenvolvimento deste trabalho, com foco em infraestrutura on-premise, práticas de monitoramento de TI e a ferramenta Centreon. .

2.1 Infraestrutura de TI On-Premise

A infraestrutura on-premise refere-se ao modelo tradicional de gerenciamento de recursos de TI, no qual servidores e demais equipamentos estão localizados fisicamente nas dependências da organização. Segundo Weiss (2020), esse modelo proporciona maior controle sobre dados e sistemas, sendo frequentemente adotado em ambientes com exigências rigorosas de segurança e conformidade legal.

"A infraestrutura on-premise é uma abordagem em que todos os recursos de hardware e software estão sob o controle direto da organização, o que pode oferecer vantagens em termos de personalização e segurança"(Weiss, 2020, p. 45).

Apesar de suas vantagens, ambientes on-premise apresentam desafios, como custos elevados de manutenção, necessidade de pessoal especializado e maior tempo de resposta para escalabilidade (Weiss, 2020).

2.2 Monitoramento de Sistemas de TI

O monitoramento de TI envolve a coleta contínua de métricas de desempenho, disponibilidade e segurança de recursos computacionais. Tanenbaum e Bos (2019) destacam que, sem sistemas de monitoramento adequados, as organizações ficam vulneráveis a falhas inesperadas, impactando a continuidade dos negócios.

"Sistemas distribuídos exigem uma abordagem de monitoramento robusta para garantir confiabilidade e detecção de falhas em tempo real"(Tanenbaum; Bos, 2019, p. 242).

O monitoramento eficaz permite a antecipação de problemas, redução do tempo médio de recuperação (MTTR) e melhor visibilidade operacional (Tanenbaum; Bos, 2019).

2.3 Alarmes e Notificações em Ambientes de TI

Os sistemas de alarmes e notificações ampliam as capacidades do monitoramento, alertando automaticamente as equipes de TI sobre eventos críticos. Conforme Kim et al. (2018), a configuração de alarmes com limiares adequados é essencial para uma gestão proativa, evitando respostas reativas que podem agravar o impacto de incidentes.

"A implementação de um sistema de alarmes com regras bem definidas é essencial para transformar o monitoramento de TI em uma prática realmente proativa"(Kim; Park; Lee, 2018, p. 77).

Em ambientes sem alarmes configurados, problemas só são detectados após repercussões no usuário final, comprometendo a confiabilidade dos serviços (Kim; Park; Lee, 2018).

2.4 A Ferramenta Centreon

Centreon é uma plataforma de monitoramento open-source que permite supervisionar servidores, redes, aplicações e serviços em tempo real. Sua arquitetura modular oferece recursos como:

- Dashboards e painéis em tempo real;
- Configuração flexível de métricas e alarmes;
- Integração por meio de plugins, SNMP e agentes dedicados;
- Geração de relatórios e análise histórica.

Estudos de caso e a documentação oficial destacam a flexibilidade do Centreon para ambientes corporativos e públicos, sendo sua adoção estratégica em organizações que buscam visibilidade centralizada sem custos de licenciamento adicionais (Tannenbaum; Bos, 2019; Kim; Park; Lee, 2018).

2.5 MTTR - Mean Time to Repair

O conceito de *MTTR* (Mean Time to Repair), ou Tempo Médio para Reparo, é uma métrica amplamente utilizada na área de gerenciamento de infraestrutura de TI e operações de sistemas para mensurar a eficiência dos processos de correção de falhas. Essa métrica indica o tempo médio que uma equipe leva para identificar, diagnosticar e corrigir um problema após sua ocorrência.

Segundo Weibull (2020), o MTTR é essencial para avaliar a confiabilidade operacional de sistemas complexos, especialmente em ambientes corporativos ou governamentais que dependem fortemente da disponibilidade contínua de serviços.

Em um contexto de monitoramento como o implementado com o Centreon, essa métrica permite avaliar o quanto eficazes estão os alertas e os fluxos de atendimento em reduzir os tempos de indisponibilidade. Como discutido por Crosby (2021), um sistema de monitoramento eficiente deve não apenas alertar sobre falhas, mas também fornecer meios para que o tempo entre a detecção do problema e sua solução seja minimizado, otimizando o MTTR.

A redução do MTTR tem impactos diretos na continuidade dos serviços e na percepção de confiabilidade da infraestrutura. Quanto menor o MTTR, maior a capacidade da organização em responder rapidamente a incidentes críticos, o que está alinhado com os princípios da Governança de TI descritos pelo ITIL (Axelos, 2019).

Kim, Park e Lee (2018) destaca ainda que uma das funções primordiais de sistemas de alerta bem configurados é exatamente permitir a rápida detecção e correção de falhas, impactando positivamente métricas como MTTR e MTBF (Mean Time Between Failures), que em conjunto oferecem uma visão abrangente sobre a resiliência de um sistema.

2.6 Hosts e Serviços no Centreon

No contexto do monitoramento de infraestrutura com o Centreon, os conceitos de hosts e serviços são fundamentais para o funcionamento da ferramenta.

Um host representa qualquer equipamento ou sistema que será monitorado, como servidores físicos, máquinas virtuais, roteadores, switches, ou sistemas em nuvem. Cada host é identificado por um nome e um endereço IP ou hostname, sendo o ponto de partida para configurar o monitoramento (Centreon Team, 2023).

Já os serviços são os elementos que descrevem o que está sendo monitorado em um host. Um serviço pode ser, por exemplo, o uso de CPU, espaço em disco, estado de uma porta de rede, tempo de resposta de uma aplicação, ou qualquer métrica que o administrador deseje acompanhar. Os serviços são associados diretamente a hosts e cada um possui um comando de verificação, um intervalo de checagem e estados possíveis (OK, WARNING, CRITICAL, UNKNOWN) (Team, 2022).

O Centreon oferece flexibilidade para criação de modelos de serviços (service templates), permitindo reutilização de parâmetros comuns entre diferentes serviços, além de herança de macros e ajustes refinados de escalonamento de alertas.

A configuração eficiente de hosts e serviços permite uma visibilidade granular

do ambiente monitorado, o que é essencial para a detecção proativa de falhas e para a implementação de alarmes inteligentes, como foi proposto neste trabalho.

2.6.1 Estados de Monitoramento: OK, WARNING, CRITICAL e UNKNOWN

No Centreon, cada verificação de serviço ou host resulta em um estado, que reflete a condição operacional daquele item no momento da checagem. Os estados são padronizados e amplamente utilizados em ferramentas de monitoramento baseadas no Nagios Core, como o próprio Centreon (Team, 2022).

- **OK:** Indica que o serviço está funcionando conforme o esperado, dentro dos limites normais e aceitáveis. É o estado ideal.
- **WARNING:** Sinaliza uma condição intermediária de alerta. O serviço está operando, mas com alguma anomalia ou valor fora do ideal, embora ainda funcional.
- **CRITICAL:** Representa uma falha ou degradação severa. O serviço está comprometido e requer ação imediata.
- **UNKNOWN:** Indica que a ferramenta não conseguiu determinar o estado do serviço. Pode ocorrer devido a problemas de configuração, ausência de resposta ou comandos mal definidos.

O uso correto e a interpretação desses estados permitem a configuração de alarmes inteligentes, priorização de incidentes e resposta proativa a falhas. Além disso, esses estados são essenciais para alimentar dashboards, relatórios e fluxos de notificação (Souza, 2020; Staahl, 2020).

2.7 Práticas de Monitoramento Proativo

Monitoramento proativo refere-se à capacidade de antecipar falhas por meio da análise contínua de indicadores e métricas, reduzindo o MTTR e aumentando a disponibilidade dos serviços. Tanenbaum e Bos (2019) argumentam que essa abordagem fortalece a resiliência da infraestrutura, fundamental em ambientes que suportam operações críticas.

3 DESENVOLVIMENTO

A implementação da solução de monitoramento e alarmes proposta neste trabalho foi realizada considerando as especificidades da infraestrutura da empresa pública Prodater, bem como a ferramenta de monitoramento Centreon, já utilizada pela instituição. Este capítulo apresenta de forma detalhada a metodologia aplicada, as etapas da implementação, as decisões técnicas envolvidas e os resultados práticos alcançados.

3.1 Contexto da Implementação

A escolha pela ferramenta Centreon foi motivada pela sua pré-existência na infraestrutura da Prodater, o que tornou mais viável sua continuidade e aprimoramento do que a adoção de uma nova solução. O Centreon é uma ferramenta de código aberto robusta para monitoramento de redes, servidores e serviços (Centreon Team, 2023). Sua arquitetura modular e capacidade de personalização permitem que seja adaptada a diversos ambientes corporativos, incluindo instituições públicas.

Devido à natureza pública da Prodater e à política interna de terceirização dos serviços de monitoramento, o acesso administrativo à instância de produção do Centreon é limitado. Por essa razão, a aplicação prática do estudo de caso foi inicialmente desenvolvida em um ambiente local controlado, com uma instalação própria do Centreon. Esta estratégia permitiu total controle sobre o sistema, possibilitando a realização de testes, personalizações e configurações sem risco à operação em produção.

3.2 Instalação Local do Centreon

A instalação do Centreon foi realizada em um servidor virtual Linux utilizando o Oracle OS 8 como sistema operacional. Seguindo a documentação oficial da ferramenta (Centreon Team, 2023), foram configurados os componentes principais: motor de monitoramento (Nagios), banco de dados MariaDB, web server Apache e as interfaces web do Centreon.

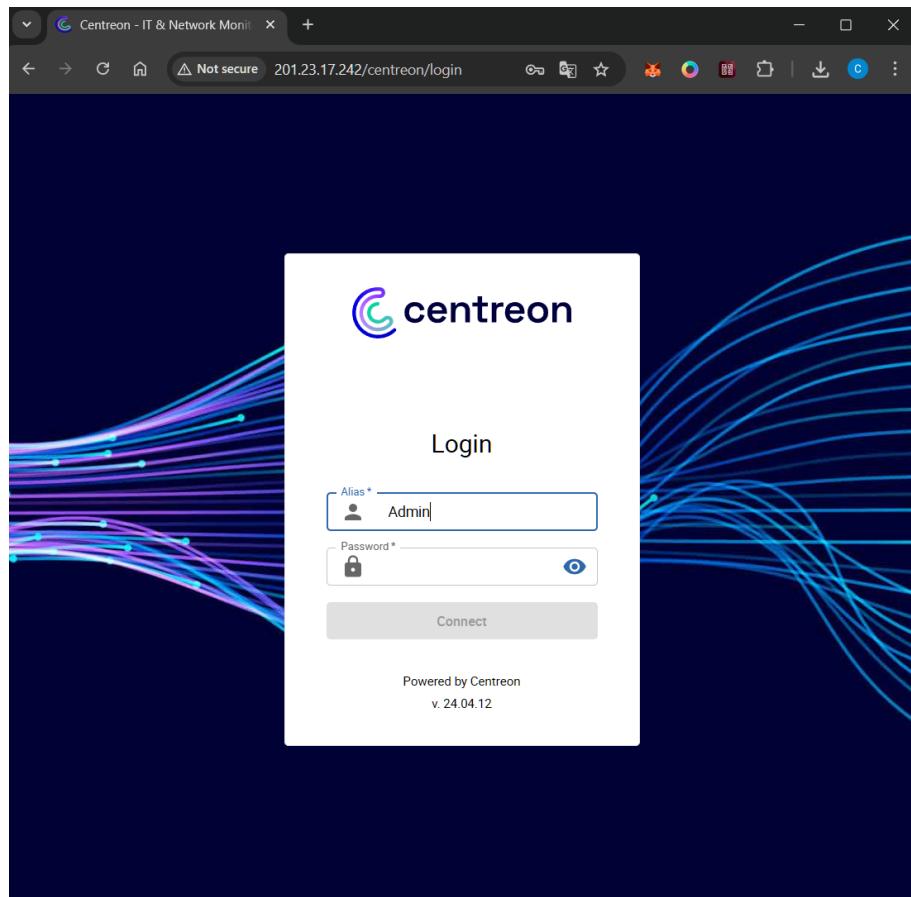
A instalação do Centreon em ambiente local teve como propósito permitir a total autonomia do pesquisador na configuração e testes da solução de alarmes. Durante o processo, foi necessário realizar ajustes no firewall, configurar os repositórios de pacotes e definir as permissões adequadas para os serviços. Essa etapa foi fundamental para garantir a segurança e a estabilidade do ambiente de testes, conforme boas práticas de administração de servidores Linux (Morimoto, 2019).

Foram seguidos os seguintes passos principais:

- Atualização do sistema operacional e dependências;
- Instalação do banco de dados MariaDB e do Apache;
- Configuração do PHP com as extensões exigidas pelo Centreon;
- Importação do repositório Centreon e instalação via YUM;
- Execução do instalador web para finalizar a configuração inicial.

Após a instalação, foi realizado o login com a conta administrativa padrão e iniciada a configuração dos serviços e hosts a serem monitorados.

Figura 1 – Instalação completa e login admin



Fonte: elaborado pelo autor (2025)

3.3 Configuração do Sistema de Alarmes

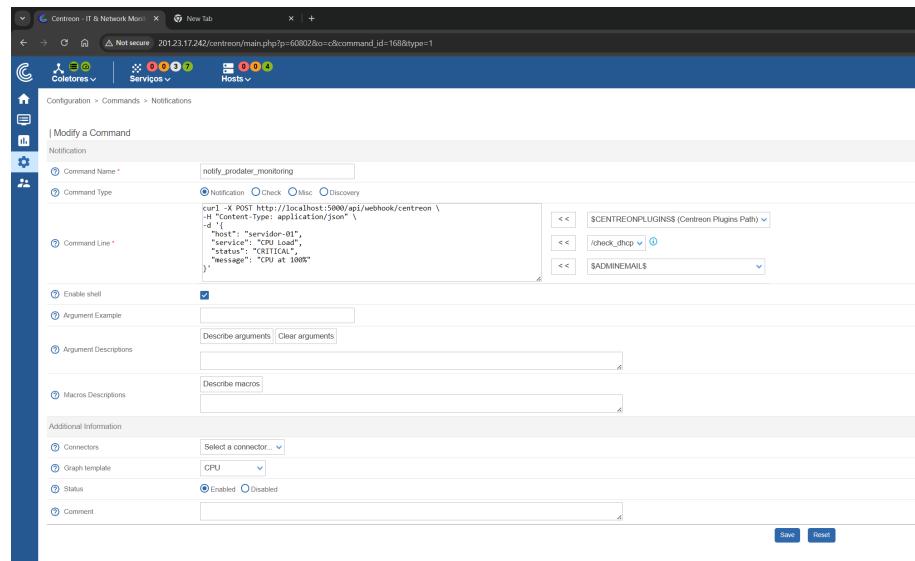
Com o ambiente local em funcionamento, foi possível configurar o sistema de alarmes do Centreon. Essa etapa incluiu a definição de serviços a serem monitorados

(como CPU, uso de disco, memória, disponibilidade de rede e serviços web), bem como os respectivos limites que disparam alertas nos níveis **WARNING** e **CRITICAL**, de acordo com as boas práticas de monitoramento (Souza, 2020).

foram configurados os hosts e serviços a serem monitorados, simulando a estrutura da rede real da Prodater. Essa simulação foi importante para validar o comportamento do sistema e identificar melhorias que pudessem ser posteriormente aplicadas na instância de produção.

Cada serviço foi vinculado a um host específico e configurado com comandos personalizados de checagem. Por exemplo, para o monitoramento de uso de CPU, definiu-se o limite de 70 % para alerta **WARNING** e 90% para **CRITICAL**.

Figura 2 – Notificação personalizada para envio de chamda de API quando acionado o alarme

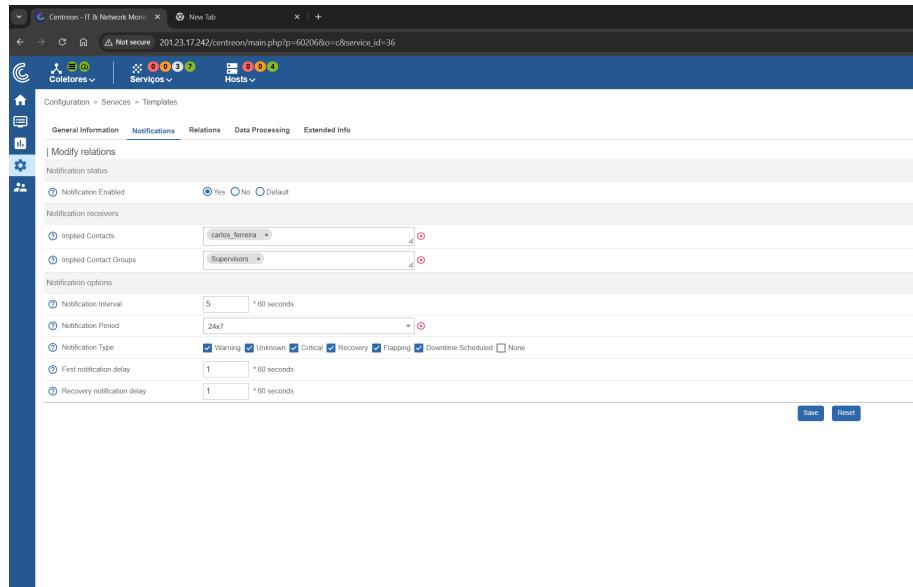


Fonte: elaborado pelo autor (2025)

3.4 Definição de Limites para os Alarmes

Os alarmes foram configurados com base em templates de serviços como uso de CPU, memória, espaço em disco, disponibilidade de serviços de rede e status de interfaces. A criticidade de cada alerta foi definida conforme parâmetros do ITIL, priorizando os que impactam diretamente nos serviços públicos oferecidos pela instituição (Silva, 2021).

Figura 3 – Configuração dos serviços via template



Fonte: elaborado pelo autor (2025)

A definição dos limites foi baseada em literatura técnica e manuais de operação de infraestrutura (Weiss, 2020). O objetivo foi garantir que os alarmes fossem disparados apenas em situações relevantes, evitando falsos positivos e notificações excessivas. Os critérios foram:

- **Uso de CPU:** WARNING a partir de 70%, CRITICAL acima de 90%;
- **Uso de memória:** WARNING a partir de 75%, CRITICAL acima de 90%;
- **Espaço em disco:** WARNING a partir de 80%, CRITICAL acima de 95%;
- **Tempo de resposta HTTP:** WARNING acima de 2s, CRITICAL acima de 5s.

Esses parâmetros foram configurados diretamente nos templates de serviços e testados com dados reais, gerando alertas simulados para verificação da eficiência do sistema.

3.5 Transição para Ambiente de Produção

Com a validação da solução local, os ajustes e templates de configuração foram transferidos para o ambiente de produção da Prodater, respeitando as políticas e permissões de acesso fornecidas pela empresa terceirizada responsável pelo ambiente do Centreon. A experiência obtida no ambiente local permitiu uma migração eficiente, segura e alinhada aos objetivos iniciais do projeto.

Após a validação dos testes locais e ajustes nos alarmes, as melhorias foram documentadas e repassadas à equipe terceirizada responsável pelo ambiente de produção do Centreon na Prodater. Com base nesse levantamento, iniciou-se uma colaboração para aplicar gradualmente as mudanças no ambiente produtivo, respeitando os fluxos de mudança e os procedimentos de homologação internos.

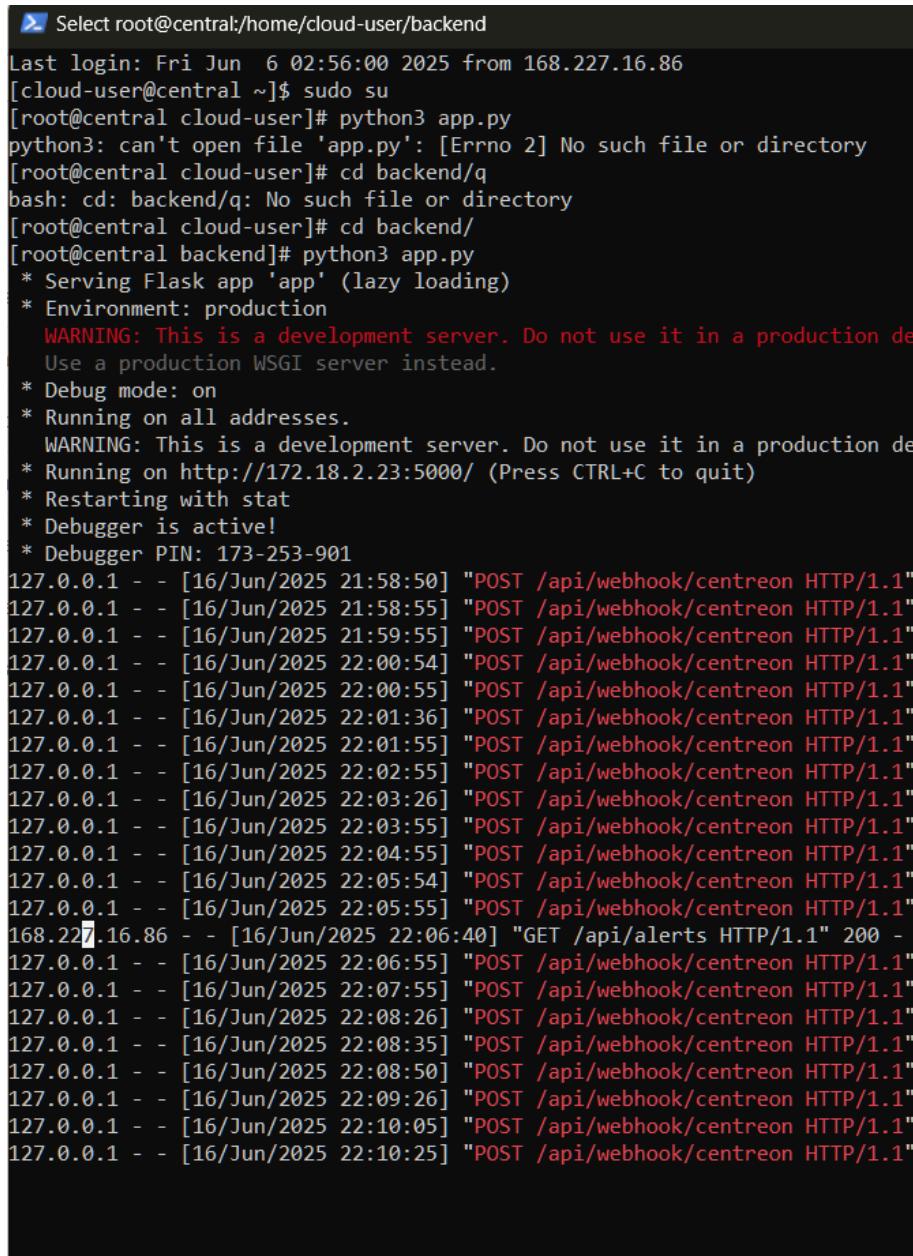
Essa abordagem garantiu maior segurança à operação e reduziu o risco de indisponibilidade dos sistemas monitorados. Além disso, possibilitou a transferência de conhecimento técnico à equipe da Prodater sobre as melhores práticas na configuração de alarmes, notificações e análise de eventos críticos (Paes, 2022).

3.6 Resultados

Durante a fase prática do projeto, foi realizado um experimento no ambiente de testes visando validar uma proposta de integração entre o sistema de monitoramento Centreon e uma interface de acompanhamento de notificações de alarmes. Para isso, foi desenvolvida uma API com o objetivo de receber, processar e exibir notificações geradas pelo Centreon.

Essa API foi configurada para ser acionada automaticamente sempre que uma notificação de alarme fosse gerada, seja em decorrência de um serviço ou host monitorado que entrou em estado anômalo (como *WARNING*, *CRITICAL* ou *UNKNOWN*). A chamada da API contém informações essenciais como o nome do host afetado, o serviço relacionado e o estado atual da verificação. Esses dados são então registrados em uma base de dados interna.

Figura 4 – Chamadas realizadas na api pelo Centreon em cada envio de notificação

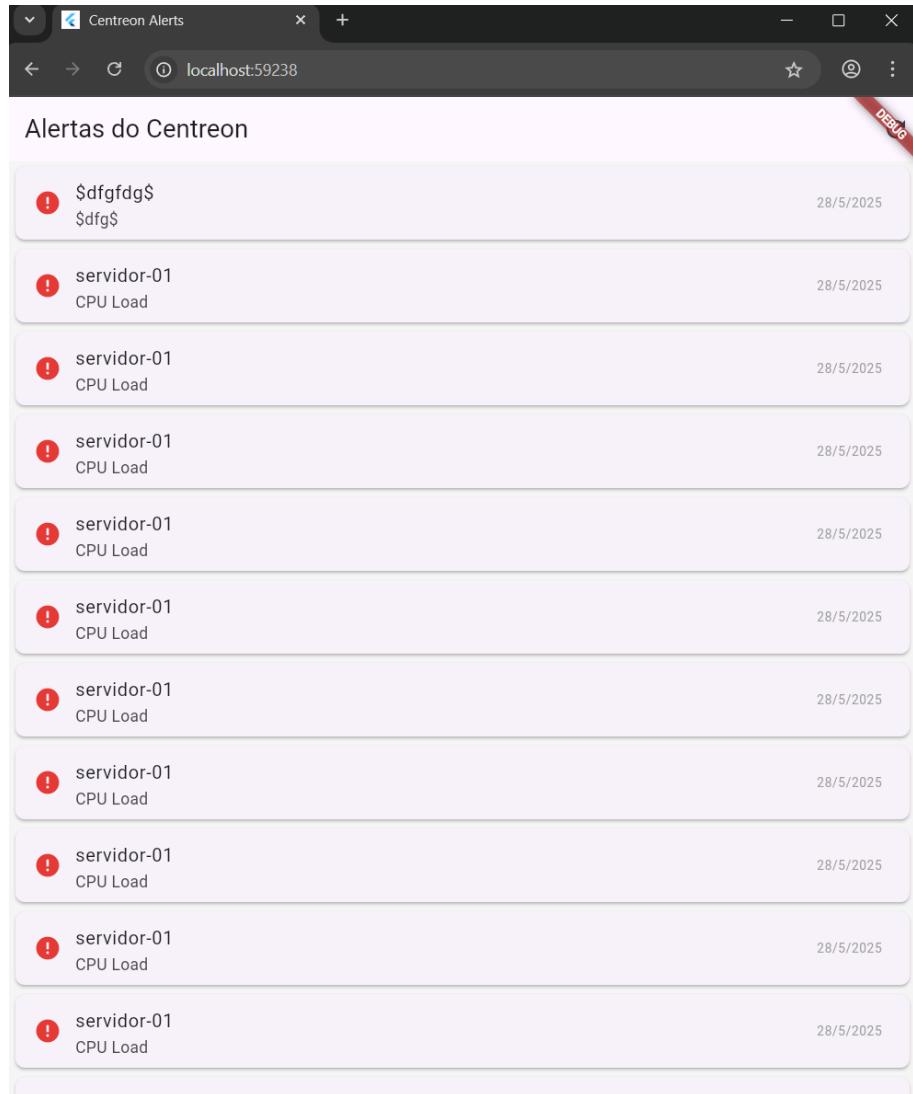


```
➤ Select root@central:/home/cloud-user/backend
Last login: Fri Jun  6 02:56:00 2025 from 168.227.16.86
[cloud-user@central ~]$ sudo su
[root@central cloud-user]# python3 app.py
python3: can't open file 'app.py': [Errno 2] No such file or directory
[root@central cloud-user]# cd backend/q
bash: cd: backend/q: No such file or directory
[root@central cloud-user]# cd backend/
[root@central backend]# python3 app.py
  * Serving Flask app 'app' (lazy loading)
  * Environment: production
    WARNING: This is a development server. Do not use it in a production de
    Use a production WSGI server instead.
  * Debug mode: on
  * Running on all addresses.
    WARNING: This is a development server. Do not use it in a production de
  * Running on http://172.18.2.23:5000/ (Press CTRL+C to quit)
  * Restarting with stat
  * Debugger is active!
  * Debugger PIN: 173-253-901
127.0.0.1 - - [16/Jun/2025 21:58:50] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 21:58:55] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 21:59:55] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:00:54] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:00:55] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:01:36] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:01:55] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:02:55] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:03:26] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:03:55] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:04:55] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:05:54] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:05:55] "POST /api/webhook/centreon HTTP/1.1"
168.227.16.86 - - [16/Jun/2025 22:06:40] "GET /api/alerts HTTP/1.1" 200 -
127.0.0.1 - - [16/Jun/2025 22:06:55] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:07:55] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:08:26] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:08:35] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:08:50] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:09:26] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:10:05] "POST /api/webhook/centreon HTTP/1.1"
127.0.0.1 - - [16/Jun/2025 22:10:25] "POST /api/webhook/centreon HTTP/1.1"
```

Fonte: elaborado pelo autor (2025)

Em conjunto com a API, foi desenvolvido um *frontend* simples, funcional e responsivo, onde é possível visualizar todas as notificações recebidas do sistema Centreon. Essa interface foi projetada com o objetivo de facilitar o acompanhamento das falhas detectadas no ambiente monitorado, de forma centralizada.

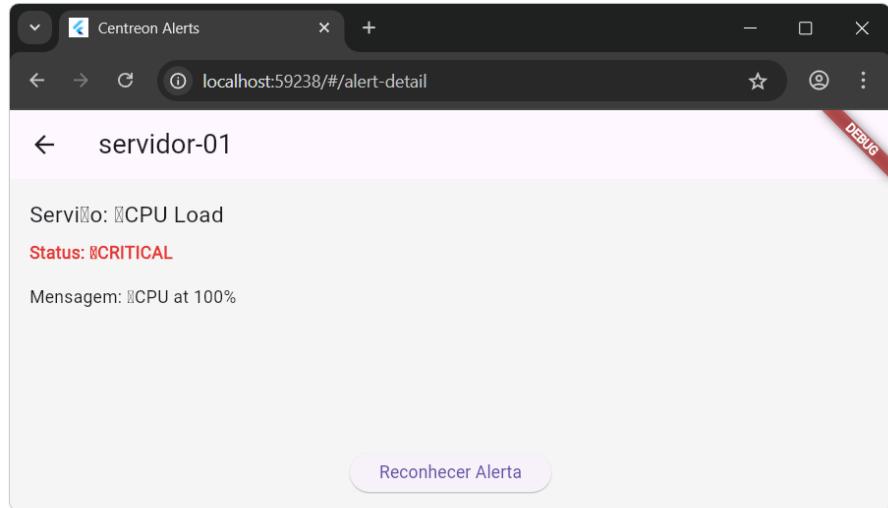
Figura 5 – Frontend com alertas recebidos



Fonte: elaborado pelo autor (2025)

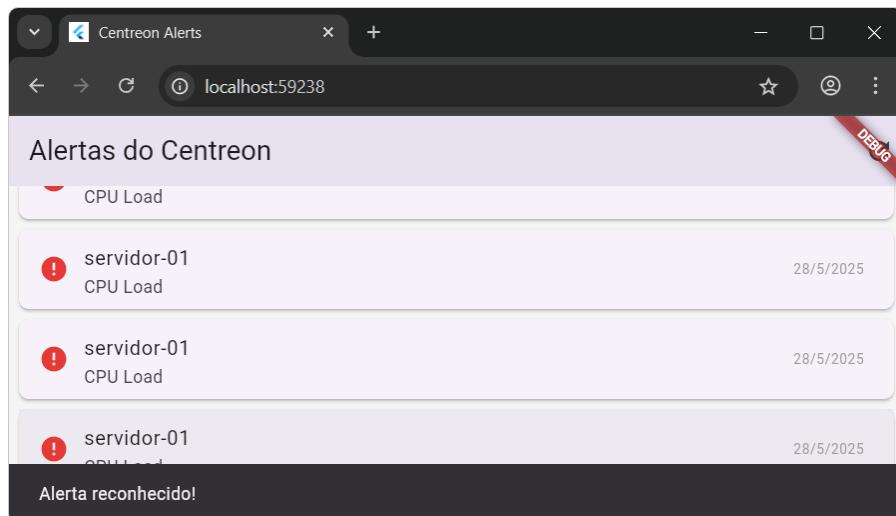
Um dos principais recursos implementados na interface foi o botão de “Tomar Conhecimento” (*Acknowledge*), presente em cada item de notificação. No contexto do Centreon e de sistemas de monitoramento em geral, “tomar conhecimento” de uma notificação significa que um operador de rede, analista ou administrador reconheceu oficialmente o problema em questão. Ao marcar uma notificação como reconhecida, o sistema registra que a falha está sendo analisada ou tratada por um responsável, impedindo o envio contínuo de novas notificações para esse mesmo evento, evitando alertas redundantes. Isso contribui significativamente para a organização das ações corretivas e reduz a sobrecarga de alertas na equipe de infraestrutura.

Figura 6 – Descrição de alarme recebido com botão de reconhecer alerta



Fonte: elaborado pelo autor (2025)

Figura 7 – Alerta reconhecido pelo usuário



Fonte: elaborado pelo autor (2025)

Com essa implementação, foi possível observar um aumento na rastreabilidade das notificações e no controle das ações tomadas frente a cada alerta gerado, otimizando o fluxo de resposta a incidentes. O ambiente de testes demonstrou que a solução proposta é tecnicamente viável e pode ser adaptada e incorporada ao ambiente produtivo da Prodater.

O *Back-end* e o *Front-end* desenvolvidos neste projeto servem como exemplo prático da flexibilidade e capacidade de customização do Centreon. Essa implementação demonstra como o sistema de monitoramento pode ser facilmente integrado a

outras soluções já existentes. A arquitetura proposta pode ser adaptada para utilizar diferentes canais de notificação, como Slack, WhatsApp, Telegram ou quaisquer outros sistemas que permitam comunicação via API, incluindo ferramentas internas de suporte e atendimento. Dessa forma, os alertas gerados pelo Centreon podem ser direcionados automaticamente para os meios mais adequados ao ambiente corporativo de cada organização.

4 CONCLUSÕES

O objetivo geral deste Trabalho de Conclusão de Curso foi analisar e demonstrar a aplicação da ferramenta Centreon para implementar um sistema eficaz de monitoramento e alarmes em um ambiente de servidor on-premise. Para atingir esse objetivo, foram estabelecidos e cumpridos os seguintes objetivos específicos: analisar as deficiências do ambiente original sem monitoramento e alarmes; estudar detalhadamente a ferramenta Centreon, incluindo suas funcionalidades e arquitetura; realizar uma implementação prática em um ambiente de testes sob controle total, e finalmente aplicar o conhecimento adquirido no ambiente produtivo da PRODATER.

A escolha pela ferramenta Centreon se deu pelo fato de já estar em uso na infraestrutura da PRODATER, o que tornou sua adoção para o projeto de alarmes mais viável e coerente com a realidade institucional. No entanto, considerando que a instância da ferramenta em produção era administrada por uma empresa terceirizada, a configuração inicial e os testes foram realizados em uma instalação própria e local, garantindo liberdade para aprender e adaptar a solução antes da aplicação em ambiente real.

4.1 Contribuições

A principal contribuição deste trabalho foi a introdução de uma abordagem proativa para a gestão de infraestrutura on-premise por meio da implementação de um sistema de monitoramento e alarmes. O estudo demonstrou que, mesmo em ambientes já operacionais, é possível melhorar significativamente a capacidade de resposta a incidentes e aumentar a disponibilidade dos serviços com a adoção de ferramentas adequadas.

Com a aplicação do Centreon, foi possível obter maior visibilidade sobre o estado da infraestrutura, detectar falhas de forma antecipada e reduzir o tempo médio de resposta a incidentes (MTTR). O trabalho também contribuiu com uma documentação prática e detalhada da configuração da ferramenta, incluindo a criação de métricas de monitoramento, alarmes e notificações.

4.2 Limitações

O principal desafio enfrentado durante a execução do projeto foi a limitação de acesso ao ambiente de produção da PRODATER, devido à gestão terceirizada da

ferramenta Centreon. Essa restrição impediu que parte das configurações e testes fossem realizados diretamente no ambiente final desde o início do projeto.

Para contornar essa limitação, optou-se por realizar a configuração inicial e os testes em um ambiente local e controlado, o que permitiu total liberdade para explorar as funcionalidades da ferramenta. Apenas após esse processo é que as melhorias puderam ser aplicadas ao ambiente real de forma segura e validada.

4.3 Trabalhos Futuros

A continuidade deste trabalho pode seguir diferentes direções, sendo recomendadas as seguintes iniciativas para trabalhos futuros:

- Ampliar o escopo da solução para incluir ambientes híbridos, permitindo o monitoramento conjunto de servidores on-premise e recursos em nuvem.
- Integrar a ferramenta com sistemas de automação para respostas automáticas a incidentes críticos.
- Elaborar programas de capacitação interna para técnicos da organização, visando maior independência na operação e configuração do sistema de monitoramento.
- Avaliar o impacto econômico da solução, mensurando ganhos em eficiência e possíveis reduções de custo operacional após a implantação.

Conclui-se que a utilização do Centreon como ferramenta de monitoramento e alarmes em ambientes on-premise é eficaz, especialmente em órgãos públicos como a PRODATER. A estratégia adotada neste trabalho pode servir como referência para outras instituições que enfrentam desafios semelhantes na gestão de sua infraestrutura de TI.

REFERÊNCIAS

- AXELOS. *ITIL Foundation: ITIL 4 Edition*. London: TSO (The Stationery Office), 2019. ISBN 9780113316076. Citado na página 17.
- Centreon Team. *Centreon Documentation*. [S.I.], 2023. Acesso em: 15 maio 2025. Disponível em: <<https://docs.centreon.com>>. Citado 2 vezes nas páginas 17 e 19.
- CROSBY, M. *Metrics and Models in Software Reliability*. [S.I.]: O'Reilly Media, 2021. Citado na página 17.
- KIM, J.-H.; PARK, J.-W.; LEE, Y.-K. An alert system for monitoring it infrastructures based on machine learning. *The Journal of Supercomputing*, v. 74, n. 10, p. 5155–5173, 2018. Citado 2 vezes nas páginas 16 e 17.
- MORIMOTO, C. E. *Servidores Linux: Guia Prático*. 6. ed. [S.I.]: Sul Editores, 2019. Citado na página 19.
- PAES, G. *Implantação de Sistemas de Monitoramento em Ambientes Corporativos*. 2022. Monografia (Bacharelado em Sistemas de Informação) – Universidade Federal de Uberlândia. Disponível sob solicitação acadêmica. Citado na página 23.
- SILVA, T. *Gestão de TI no Setor Público: Desafios e Boas Práticas*. [S.I.], 2021. Citado na página 21.
- SOUZA, B. *Monitoramento com Nagios: Soluções para infraestrutura de TI*. São Paulo: Novatec Editora, 2020. ISBN 978-85-7522-781-9. Citado 2 vezes nas páginas 18 e 21.
- STAABL, A. *Understanding Service States in Monitoring Systems*. 2020. <<https://www.monitoring-plugins.org/doc/guidelines.html>>. Acesso em: 10 jun. 2025. Citado na página 18.
- TANENBAUM, A. S.; BOS, H. *Modern Operating Systems*. 4. ed. [S.I.]: Pearson, 2019. Citado 2 vezes nas páginas 15 e 16.
- TEAM, C. *Centreon Administrator Manual*. [S.I.], 2022. Acesso em: 10 jun. 2025. Disponível em: <<https://docs.centreon.com/docs/administration/monitoring/configure-objects/>>. Citado 2 vezes nas páginas 17 e 18.
- WEIBULL, W. *Reliability and Maintenance Metrics*. [S.I.]: Springer, 2020. Citado na página 17.
- WEISS, A. *Infraestrutura de TI: planejamento, implantação e gerenciamento*. [S.I.]: Novatec Editora, 2020. Citado 2 vezes nas páginas 15 e 22.