UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CAMPUS PATO BRANCO
DEPARTAMENTO DE INFORMÁTICA
CURSO DE ENGENHARIA DE COMPUTAÇÃO

Relatório Final de Estágio Curricular Obrigatório

Relatório Final de Estágio apresentado à UTFPR como requisito parcial da disciplina de Estágio Curricular Obrigatório do Curso de Engenharia de Computação.

Pato Branco
2023

Edinei da Motta Martinello

Relatório Final de Estágio Curricular Obrigatório

Relatório Final de Estágio apresentado como requisito parcial da disciplina de Estágio Curricular Obrigatório do Curso de Engenharia de Computação.

Orientador(a): Me. Adriano Serckumecka

Pato Branco

2023

Resumo

Este documento tem como finalidade descrever as tarefas realizadas durante a realização do estágio curricular obrigatório que aconteceu no período de março de 2023 a dezembro de 2023 na empresa WEG Equipamentos Elétricos S.A., multinacional brasileira, na Seção de Tecnologia de Infraestrutura. O projeto me deu a oportunidade de explorar junto a equipe de redes, uma área pouco conhecida, mas bastante relevante para o dia a dia, a qual é o fluxo de dados entre equipamentos de rede, aos quais são relevantes para compreensão das aplicações em produção e apoio para identificação de algum problema que esteja acontecendo e não tenha visibilidade. Durante esse processo, pude compreender a arquitetura de rede, identificar oportunidades de melhoria, principais aplicações e servidores, elaborar dashboard sobre os dados coletados. Junto a equipe de servidores apoie diretamente no desenvolvimento e implantação de uma automação de criação/clone de servidores virtuais. Durante esse processo, pude compreender servidores, virtualização, arquitetura de discos LVM, desenvolvendo automações uteis ao dia a dia. Além da evolução no conhecimento técnico foi possível conhecer mundo corporativo o que torna o estágio ainda mais produtivo.

Palavras-chave: Redes. Infraestrutura de Redes. Análise de Dados. Servidores. Automação de Infraestrutura.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

DAINF – Departamento Acadêmico de Informática
LAN – *Local Area Network*
MAN – *Metropolitan Area Network*
WAN – *Wide Area Network*
MPLS – *Multi Protocol Label Switching*
RIP – *Routing Information Protocol*
OSPF – *Open Shorting Path First*
BGP – *Border Gateway Protocol*
SNMP – *Simple Network Management Protocol*
NMS – *Network Management Station*
MIB – *Management Information Bases*
OID – *Object Identifier*
BI – *Business Intelligence*
VM – *Virtual Machine*
AWX – *Ansible Web eXperience*
LVM – *Logical Volume Manager*
ID – Identificador
API – Interface de programação de aplicações

SUMÁRIO

1 IDENTIFICAÇÃO DO ESTÁGIO

1.1 Aluno

Nome: Edinei da Motta Martinello
Código do aluno na UTFPR: 2009676

1.2 Empresa

Nome: Weg Equipamentos Elétricos S/A
Razão Social: S/A
CNPJ: 07.175.725/0001.60
Área de atuação: Motores e Equipamentos Elétricos
Endereço: Av. Pref. Waldemar Grubba, 3000
Bairro: Vila Lalau
CEP: 89256-900
Cidade: Jaraguá do Sul
Estado: SC
Nome do responsável pelos estágios na empresa: Michel Simon

1.3 Estágio

Área de atuação: Redes Industriais
Setor: Tecnologia de Infraestrutura
Data de início: 06/03/2023
Data de conclusão: 22/12/2023
Período do dia do estágio: 8h
Carga horária semanal: 40h

1.4 Supervisor de Estágio na Empresa

Nome: Tales Marcos Cardoso
Formação acadêmica na graduação: Sistemas de Informação
Cargo: Gerente da Seção
Departamento ou setor que trabalha: Tecnologia de Infraestrutura
Responsabilidades do departamento ou setor que trabalha: Projetos, Segurança e Sustentação da Rede/Servidores.

1.5 Orientador de Estágio da Universidade

Nome: Adriano Serckumecka
Formação acadêmica na graduação: Tecnologia em Análise e Desenvolvimento de Sistema
Cargo: Professor
Departamento: DAINF

2 INTRODUÇÃO

Dentro da rede corporativa (LAN/MAN), existem equipamentos que suportam a leitura do tipo de tráfego que está sendo transmitido. Esses equipamentos podem ser configurados para melhorar a visibilidade local e fornecer informações importantes, como, por exemplo, quais são os clientes que mais ‘falam’ e quais são os servidores mais acessados, incluindo apoio para identificação de algum problema que esteja acontecendo e não tenha visibilidade. Dentre as etapas desenvolvidas estão: validar as topologias de rede configuradas na LAN/MAN, identificar oportunidades de melhoria nas topologias, definir os ambientes que serão monitorados e implementar visibilidade nos equipamentos que suportarem a configuração.

2.1 Atividades Desenvolvidas no Estágio

- Observabilidade de Dados na Rede – Teórico;
- Treinamento sobre Redes;
- Métricas de Rede;
- Protocolo SNMP;
- Mapeamento da topologia;
- Observabilidade da Dados na Rede – Aplicação;
- Coleta, Tratamento e Visualização dos Dados;
- Treinamentos Automações de Infraestrutura;
- Verificação de portas livres em switches;
- Atualização de aplicações;
- Automatização no processo de criação e clone de servidor virtual;
- Descoberta automática da topologia Cisco;
- Contagem de Mac Address;
- Backup de configuração;
- Informações das portas dos switches.

3 A EMPRESA

A WEG é uma empresa brasileira com um longo histórico no setor de tecnologia elétrica e automação. Fundada em 1961, a empresa tem como objetivo principal oferecer soluções inovadoras e eficientes para o mercado global, abrangendo diversos setores industriais e comerciais.

A missão da WEG é fornecer produtos e serviços de alta qualidade no campo de energia elétrica, automação e eficiência energética. Sua atuação é delimitada pela busca constante por excelência e liderança no mercado, contribuindo para o progresso sustentável.

A visão da empresa é se tornar uma referência mundial em tecnologias elétricas, impulsionando o desenvolvimento econômico e social por meio de soluções inovadoras e sustentáveis. A WEG aspira a ser reconhecida como líder global em seu segmento, estabelecendo padrões de excelência e contribuindo para um futuro mais eficiente e ecologicamente responsável.

Os valores e princípios da WEG incluem o compromisso com a ética, a integridade e a responsabilidade social. A empresa valoriza a inovação, a busca pela qualidade, o respeito às pessoas e ao meio ambiente, assim como a busca constante por melhorias em suas operações e processos. A cultura da empresa é pautada na colaboração, na valorização dos colaboradores e na dedicação ao cliente, refletindo seu comprometimento com a excelência em todas as áreas de atuação, (Web, 2023).

4 FUNDAMENTOS TEÓRICOS

4.1 Métricas de Rede

Métricas de rede são medidas quantitativas usadas para avaliar e monitorar o desempenho e a confiabilidade de uma rede de computadores. Essas métricas fornecem informações valiosas sobre vários aspectos do comportamento da rede, como velocidade, uso de largura de banda, latência, perda de pacotes e outros indicadores chave de desempenho (KPIs) da rede, como por exemplo:

- *Packet Loss*: Perca de um ou mais pacotes enquanto navegam pela rede de computadores durante uma transmissão de dados;
- *Jitter*: Variação da latência entre pacotes;
- Latência: Tempo que um pacote de dados leva para ser transmitido;
- Erros e descartes de pacotes na interface: Dentre as causas, incluem: intensidade de sinal inadequada no destino, interferência natural ou provocada pelo homem, ruído excessivo do sistema, corrupção de software ou nós de rede sobrecarregados;
- Consumo de link: Quantidade de banda utilizada dentre a quantidade disponível;
- *Top users*: Principais endereços que trafegam maior volume de dados dentre uma aplicação;
- Consumo por aplicação: Volume de dados trafegados dentre o todo.

Monitorando e analisando essas métricas de rede, os administradores podem identificar gargalos de desempenho, diagnosticar problemas e otimizar as configurações da rede para melhorar o desempenho da rede, reduzir o tempo de inatividade e proporcionar uma melhor experiência ao usuário (Lamberti, 2023).

4.2 Protocolo SNMP

O SNMP é um protocolo de gerenciamento de rede que oferece uma interface unificada para diversos dispositivos conectados à mesma rede. Ele possibilita a comunicação e troca de dados entre dispositivos em uma rede, permitindo identificação, monitoramento de desempenho, rastreamento de mudanças e acompanhamento em tempo real do status dos dispositivos, como roteadores, switches, impressoras e *firewalls*.

O protocolo opera em camadas e coleta e organiza dados por meio de endereços IP. Ele é adequado para empresas de todos os tamanhos, oferecendo monitoramento direto e compatibilidade com uma variedade de dispositivos. O SNMP é composto por diferentes elementos, incluindo o Sistema de Gerenciamento de Rede (NMS), que gerencia os componentes de rede, o Agente SNMP, que executa operações solicitadas pelo MIB (Base de

Informações Gerenciais) no *hardware* ou serviço monitorado, e o Dispositivo Gerenciado, que é um nó na rede contendo o agente SNMP e o MIB.

O Gerenciador SNMP é uma estação de gerenciamento centralizada que se comunica com dispositivos que possuem o agente SNMP. Ele envia solicitações e recebe respostas periodicamente, realizando funções como envio de consultas, recebimento de respostas, definição ou alteração de variáveis e reconhecimento de eventos assíncronos.

O Agente SNMP é um software presente em dispositivos de rede, responsável por coletar dados do ambiente local, armazenar e recuperar informações no MIB, notificar o gerenciador sobre eventos e atuar como um proxy para dispositivos não SNMP gerenciáveis.

O SNMP utiliza portas, sendo a Porta 161 usada para envio de solicitações do NMS ao agente SNMP, e a Porta 162 para o agente SNMP enviar *traps* ou informações ao NMS.

No SNMP, o dispositivo gerenciado é um nó de rede contendo um agente SNMP. O MIB é uma estrutura de dados em árvore que armazena valores de dispositivos de rede, permitindo coleta, configuração e modificação de informações. Os OIDs (Identificadores de Objeto) são números usados para distinguir dispositivos na base, permitindo o acesso a objetos gerenciados por MIB.

As comunidades, presentes no SNMPv1 e SNMPv2, gerenciam os direitos de acesso. Já no SNMPv3, os usuários substituem as comunidades e pertencem a grupos com direitos de acesso atribuídos, também se destaca pela possibilidade de segurança, com criptografia.

O NMS (Sistema de Gerenciamento de Rede) é um aplicativo ou conjunto deles que possibilita o gerenciamento de componentes independentes dentro de uma estrutura de gerenciamento de rede. Ele é usado para monitorar *software* e *hardware*, registrando dados de pontos remotos para criar relatórios centralizados, (Phoenixnap, 2023).

4.3 *Logical Volume Manager* (LVM)

A arquitetura LVM, é uma camada de abstração de armazenamento para o kernel do Linux, que fornece uma maneira flexível e dinâmica de

gerenciar volumes de armazenamento. Essa arquitetura é particularmente útil em ambientes onde a capacidade de armazenamento precisa ser gerenciada de maneira eficiente e flexível, especial em situações de expansão de disco, essa flexibilidade permite que o ajuste dinâmico ocorra conforme necessário, sem a necessidade de desligar o sistema ou recriar partições, assim facilitando a expansão ou redistribuição de espaço de armazenamento, (Redhat, 2023).

Aqui estão os principais componentes da arquitetura de discos LVM:

- *Physical Volumes (PVs):*
  - São dispositivos de armazenamento físico, como discos rígidos ou partições;
  - Um ou mais PVs são agrupados para criar um grupo de volumes físicos *(Volume Group).*
- *Volume Groups (VGs):*
  - São grupos de *Physical Volumes*;
  - Podem ser expandidos adicionando mais *Physical Volumes*;
  - Dentro de um VG, você cria *Logical Volumes (LVs).*
- *Logical Volumes (LVs):*
  - São análogos às partições em sistemas de arquivos tradicionais;
  - LVs são criados dentro de *Volume Groups;*
  - Podem ser redimensionados dinamicamente.

5 ATIVIDADES DESENVOLVIDAS

O projeto realizado foi definido com o seguinte escopo: Estudar e implantar ferramenta de visibilidade de redes de computadores a qual permita identificar o comportamento das aplicações corporativas na rede local LAN e mundial WAN. O produto deste estudo permitiu:

- Identificar possibilidades de otimização das despesas com circuitos MPLS Datacenter WEG com filiais do Brasil e Exterior;
- Identificar os principais interesses de tráfego entre unidades;
- Prover visibilidade sobre os tipos de dados trafegados da rede local;

- Identificar desvios de comportamento de tráfego que possam estar impactando a experiência dos usuários.

5.1 Observabilidade de Dados na Rede – Teórica

Como atividade inicial de compreensão sobre o projeto e pré-requisito para as atividades posteriores, foi realizado estudo sobre os fundamentos teóricos de observabilidade de dados na rede, que pode ser definida como a capacidade de resolver qualquer pergunta sobre a rede de forma rápida e fácil. Dentre os eventos estudados e relacionados à observabilidade de dados na rede, pode-se destacar:

- Ganhos
  - Minimização de latência de rede;
  - Descoberta de problemas antes de causarem problemas;
  - Maior confiança nos dados.
- Oportunidades
  - Melhoria da performance dos sistemas;
  - Otimização da experiência do usuário;
  - Maior rapidez para realizar reparos.
- Riscos
  - Interceptação de dados;
  - Troca de dados;
  - Acesso à rede.
- Ferramental
  - Captura de métricas;
  - Notificação;
  - Rastreamento;
- Boas práticas
  - Monitorar o tráfego de rede e métricas de desempenho regularmente;
  - Monitorar sua infraestrutura;
  - Acompanhar novas tecnologias.

- Abrangência
    - Dispositivos de rede;
    - Servidores;
    - Acompanhamento em tempo real.

Conforme artigos relacionados: (Kentik, 2023), (William, 2023), (Positivo, 2023).

5.2 Treinamento de Redes

Em estágio inicial do projeto foram realizados treinamentos sobre redes, na plataforma (Alura, 2023), na qual pôde-se reforçar os conceitos relacionados a redes industriais e *wireless*, além de compreender seu funcionamento no ambiente de rede corporativa da empresa.
Os treinamentos realizados tiveram como foco:

- Redes *onboarding*: uma perspectiva prática;
- Redes parte 1: conceitos e prática;
- Redes parte 2: montando um projeto do cliente até o provedor de serviços;
- Redes parte 3: defina as listas de controle e políticas de acesso de usuário;
- Redes parte 4: configuração de protocolos de roteamento e IPv6;
- Redes parte 5: Wi-Fi;
- Elaboração de apresentação, sobre os tópicos abordados e contextualização com a empresa.

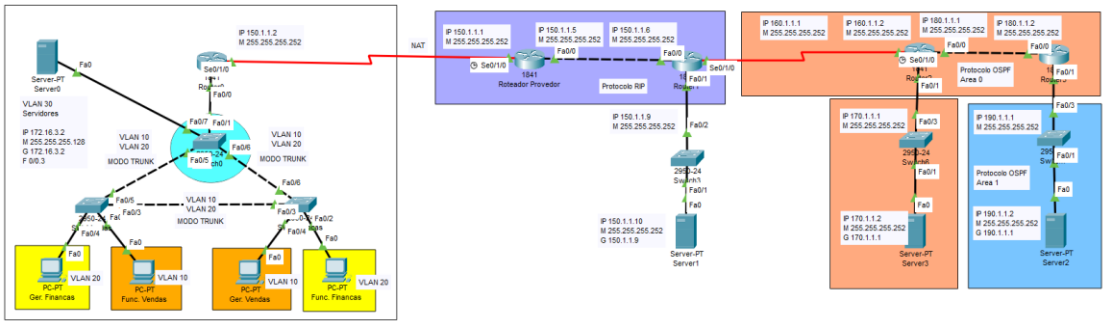
Os resultados alcançados com os treinamentos viabilizaram novos conhecimentos que puderam ser aplicados em tarefas posteriores, tendo como destaque:

- A organização da rede com os diferentes equipamentos de rede, deste o provedor de internet a conexão do usuário final, seja via cabo ou Wi-Fi
- VLAN e MODO TRUNK aplicado ao ambiente fabril;
- Redundância de conexão entre equipamentos e o uso do *Spanning Tree Protocol;*

- Protocolos de roteamento: RIP, OSPF, BGP;
- Rede Wi-Fi e a hierarquia de equipamentos;
- Aplicação e absorção de conceitos estudados realizando exemplos práticos, em ambiente de simulação usando o *Packet Tracer.*

A Figura 1 fez parte do treinamento, onde foi possível demonstrar uma infraestrutura de rede industrial, com seus equipamentos e segmentação de redes.

Figura 1 – Rede Industrial



Autor: Autoria própria

5.3 Métricas de Rede

Foram realizados estudos envolvendo as principais métricas de rede, coletando dados para análise posterior e uma melhor compreensão em ambiente de produção. Como resultado, foram identificados alguns indicadores em aplicações de interesse, que poderão ser utilizados futuramente em otimizações da rede.

5.4 Protocolo SNMP

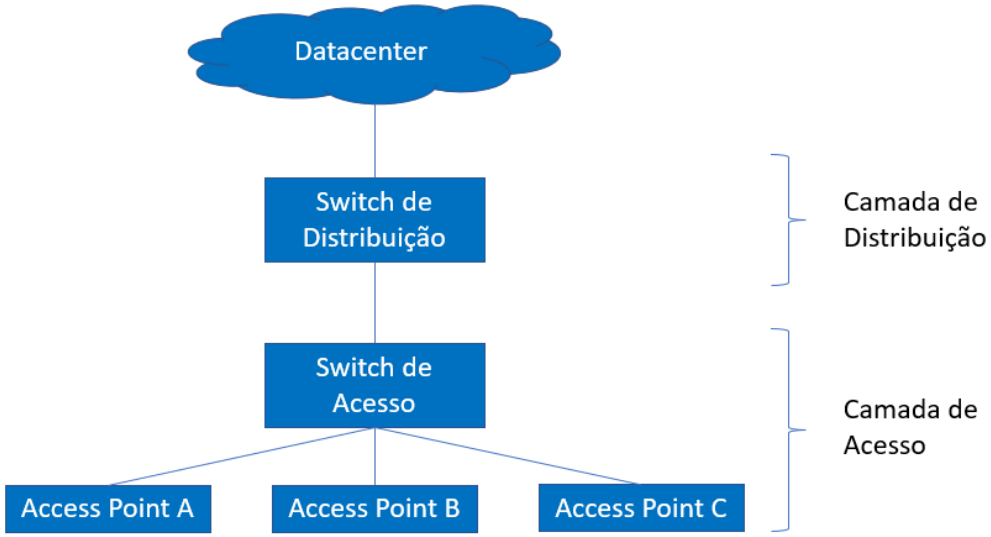
Foi realizado um estudo sobre o protocolo SNMP e suas aplicações, envolvendo a configuração de switches locais e atividades práticas, como testes de transferência de arquivos via cabo e *wireless*, monitoramento utilizando o *Wireshark*, SNMP *TrafficGrapher* e *MibBrowser*.

5.5 Mapeamento de topologia

Buscando compreender a topologia do parque fabril, foram realizados o mapeamento de topologia dos parques fabris da rede, sendo eles: Parque Fabril A, B, C, D e E.

Identificando, ilustrando equipamentos, contabilizando e classificando o número de equipamentos. Durante essa atividade, foram encontrados pontos de melhorias, seja por falta de configuração de método de acesso, descrição ou arquitetura da rede. Um exemplo de ilustração está representando na Figura 2.

Figura 2– Mapeamento de Topologia



Autor: Autoria própria

Como apresentado na Figura 2, foram ilustrados a topologia dos equipamentos nos diferentes ambientes da camada distribuição de rede, encontrando diferentes arquiteturas, alguns dos quais foram apontados para revisão de arquitetura, por motivos de otimização do ambiente.

Tendo em posse as diferentes topologias de rede, estas foram usadas para compreensão do ambiente e para definir os ambientes para serem monitorados e habilitar visibilidade nos equipamentos que suportam a configuração.

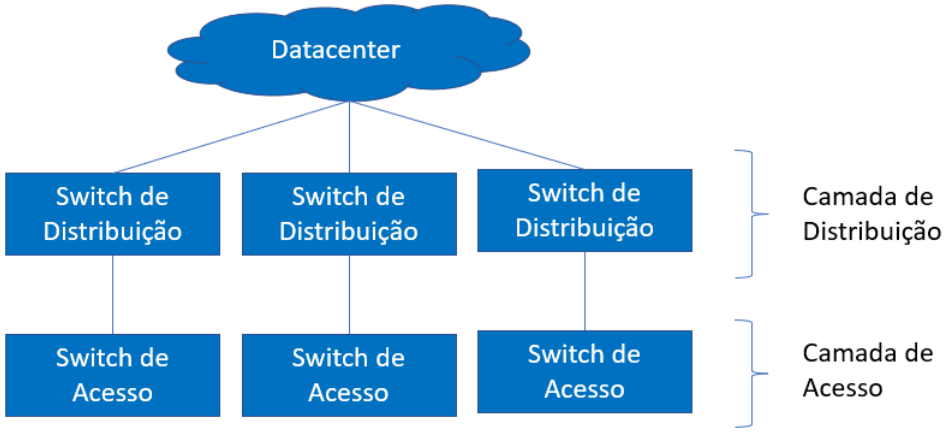
5.6 Observabilidade da Dados da Rede – Aplicação

Compreendido o funcionamento do protocolo SNMP nos equipamentos de rede e em posse das informações obtidas com o mapeamento de rede local, foram escolhidos ambientes que despertaram interesse para análise, assim, utilizando ferramenta de observabilidade, optando pelo software *Netflow Analyzer,* (Solarwinds, 2023), já consolidado e utilizado em ambiente de sustentação de rede.

Seu funcionamento ocorre através da leitura dos dados SNMP nos equipamentos de rede, que são processados pelo software e apresentados em formato de gráficos de barras ou pizza, aos quais é possível criar relatórios e alertas. Com o software, foi possível monitorar o fluxo de tráfego de rede e, assim, compreender as aplicações, protocolos, fontes, destinos, pontos de congestionamento e volume de dados.

Inicialmente foi configurado em um switch de laboratório (isolado do ambiente de produção), para compreensão do software e verificação de seu funcionamento. Após compreensão sobre o software foi habilitado em ambiente de produção, escolhendo ambientes de interesse encontrados durante o mapeamento de topologia, no qual foram habilitados em switches e roteadores, assim, compreendendo o fluxo de dados do ambiente monitorado, como: os principais transmissores, as principais conversas entre *hosts*, principais protocolos, aplicações, entre outras informações.

Figura 3 – Ambiente monitorado



Autor: Autoria própria

Em posse do domínio do software e compreensão das informações apresentadas, foram habilitados na camada de distribuição de rede, coletando o fluxo de tráfego entre a camada de distribuição e o datacenter, sendo eles: Parque Fabril A, B e C, como representado na Figura 3.

No Parque Fabril D, mesmo com orientação do fabricante apresentou resultados abaixo do esperado, assim, não entrando na análise e o Parque Fabril E, ao qual, já é monitorado pela equipe de sustentação de rede.

5.7 Coleta, Tratamento e Visualização dos Dados

Com o software habilitado nos parques fabris, foram coletados dados durante 3 semanas, 15 dias, sendo realizado downloads dos relatórios diariamente, totalizando em um *dataset* de 7,8 milhões de linhas.

Com os dados coletados do software, exportados em formato Excel, realizou-se o tratamento destes dados (data, padronização, colunas vazias, união de *dataset*, arquivamento em csv) utilizando bibliotecas do Python.

Utilizou-se informações internas da empresa para categorização das aplicações, servidores e máquinas industriais. Assim escolhendo aplicações de interesse como: File Server, Proxy Internet, SAP, Maestro e Easy.

Para melhor visualização das informações foi utilizado software de visualização de dados *Power BI*, ao qual foi realizado treinamento prévio, para compreensão da ferramenta. Assim, consolidando as informações em um dashboard para melhor visualização das informações, estas apresentadas para a equipe de projetos redes e servidores, além da equipe de segurança da informação, discutidas as informações encontradas e realizando ajustes no dashboard conforme sugerido pela equipe.

5.8 Treinamentos Automações de Infraestrutura

Durante o estágio tive a oportunidade de trabalhar com novas tecnologias, relacionadas a automações de infraestrutura de redes e servidores, foram realizados treinamentos sobre Linux, linguagem Shell Script, linguagem de automação de infraestrutura Ansible e Docker na plataforma

Alura, na qual pude aprender os conceitos relacionados a servidores, além de compreender seu funcionamento no ambiente de produção da empresa.
Os treinamentos realizados tiveram como foco:

- Ansible: sua infraestrutura como código;
- Linux Onboarding: usando a CLI de uma forma rápida e prática;
- Linux Onboarding: localizando arquivos e conteúdos;
- Linux Onboarding: obtendo e tratando informações do sistema;
- Linux Onboarding: trabalhe com usuários, permissões e dispositivos;
- Shell Scripting parte 1: scripts de automação de tarefas;
- Shell Scripting parte 2: fazendo monitoramento, agendando tarefas e backup;
- Docker: criando e gerenciando containers;
- Git e Github.

Os resultados alcançados com os treinamentos viabilizaram novos conhecimentos que puderam ser aplicados em tarefas posteriores.

5.9 Verificação de portas livres em switches

Por meio de um processo de acompanhamento do tráfego na porta dos switches é possível determinar se uma determinada porta está livre ou ocupada, esse processo ocorre realizando coletas via protocolo snmp de bytes trafegados na porta, realizando uma coleta semanal em todos os switches da rede, por consenso interno, considera-se uma porta livre de switch a qual tenha trafego igual ou decrescente no período de 4 semanas de coletas, essa informação é muito utilizada no dia a dia, pois auxilia a otimizar a utilização de todas as portas dos switches.

Até então, tido em produção, um script desenvolvido na linguagem Autoit em meados de 2008, em contrapartida, o script acabou deixando de funcionar, então desta vez, foi desenvolvido utilizando linguagem Ansible, o script, envolveu variais etapas, como cópia da lista de switches atualizada da ferramenta de governança, antes de qualquer execução, execução da tarefa de coleta de dados, execução da tarefa de verificação de portas livres com base nas coletas realizadas, envio dos dados com os resultados entre servidores, finalizando na atualização da ferramenta de monitoramento, para o novo script,

ao qual apresenta um dashboard com as informações geradas, essas sendo usadas para tomada de decisão das equipes de redes e operações.

5.10 Atualização de aplicações

Algumas aplicações internas recebem atualizações periodicamente, estas precisam parar o pool da aplicação, deixar em modo espera as filas de usuários e realizar a transferência de arquivos para os diretórios da aplicação, após isso, iniciar novamente o pool da aplicação.

O processo de transferência de arquivos entre servidores, ocorre realizando a conexão no servidor da aplicação, criando unidade de compartilhamento em cada um, realizando assim o mapeamento do diretório, posteriormente realizando a transferência dos arquivos. O sistema de compartilhamento de arquivos foi a alternativa encontrada para conseguir realizar a tarefa, no ambiente AWX, ao qual, não estava sendo possível ser desenvolvido utilizando módulos de copias de arquivos tradicionais do Windows, como por exemplo: robocopy.

AWX, uma ferramenta desenvolvida pela comunidade, utilizada para automações em servidores, a qual funciona de maneira paralela, sendo desenvolvido em Ansible e comando Power Shell.

A rotina está representada na figura 4, ao qual, após executar a rotina no ambiente AWX, ocorre a parada do pool da aplicação, posteriormente a transferência de arquivos, em seguida, a inicialização do pool da aplicação.

Figura 4 – Atualização de aplicações

Autor: Autoria própria

Essa automatização tornou possível a realização das demandas do dia a dia de maneira mais rápida e escalável, buscando minimizar o tempo da aplicação parada.

5.11 Automatização no processo de criação e clone de servidor virtual

O processo de criação/clone de servidor virtual (VM) ocorre por meio da virtualização de servidores, o qual é o processo de dividir um servidor físico em vários servidores virtuais únicos e isolados por meio de um aplicativo de software, assim cada servidor virtual pode executar seus próprios sistemas operacionais de forma independente (Vmware, 2023).

No contexto de servidores Linux, a arquitetura *Logical Volume Manager* (LVM) desempenha um papel importante na gestão do armazenamento dessas VMs, especial em situações de expansão de disco, a qual permite o ajuste dinâmico ocorra, sem a necessidade de desligar o sistema ou recriar partições, assim facilitando a expansão ou redistribuição de espaço de armazenamento, mais detalhes sobre arquitetura LVM pode ser visto na Seção 4.3.

A presente tarefa, buscou reduzir o tempo gasto da equipe de servidores na criação/clone de servidor virtual de maneira sequencial, a tarefa tem um processo longo, envolvendo vários colaboradores, seja para realizar a criação/clone de um servidor virtual, validação após criada, criação de sistema de *backup* customizado e validação de regras de *firewall*.

Processo de criação/clone de servidor virtual anterior a automação

O processo sequencial de criação/clone de servidor virtual atual, ocorre da seguinte maneira: um colaborador do departamento de infraestrutura, realiza a solicitação, por meio de um formulário desenvolvido na plataforma Service Now, informando as características da máquina, como: rede, hardware, sistema operacional, tipo de backup, função, janela de manutenção, dentre outras especificações.

Com esse formulário preenchido, gera-se um ID, consolidando todas as informações descritas pelo colaborador, posteriormente, direcionava a implantação para a equipe de servidores para realizar a criação/clone do servidor virtual. Após a implantação realizada, outro colaborador realizava a validação do servidor, seguindo um roteiro de checagem, caso seja encontrado uma inconsistência, ele realiza a correção.

O profissional Anderson Mekelburg, (Analista de Suporte/Projetos/ Servidores), destaca que: “o processo de criação/clone de servidores virtuais

era um processo manual, algumas etapas dos procedimentos por vezes eram ignoradas ou esquecidas de serem executadas. Com isso, havia problemas com relação à inconsistência de dados nas ferramentas de inventário, monitoramento, backup, entre outras tantas necessárias para a governança do ambiente de Datacenter. Além dessas inconsistências, era necessário um retrabalho de alguns técnicos e analistas para correção dessas inconsistências, o que demandava um esforço desnecessário visto que poderiam ser evitadas executando o procedimento corretamente".

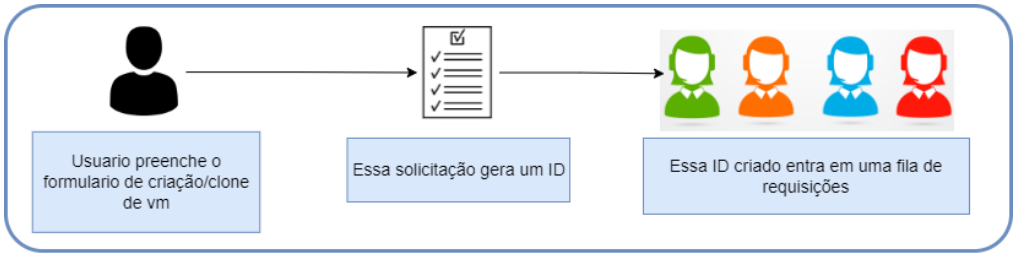
Compreendendo ser uma tarefa repetitiva para o dia a dia, e envolvendo as mesmas tarefas toda vez, buscou-se uma maneira de automatizar esse processo, desenvolvendo a arquitetura das etapas envolvidas, e a definição da ferramenta de automação nesse processo.

Processo de criação/clone de servidor virtual após a automação

Basicamente, agora, o fluxo de criação/clone de um servidor virtual, se dá da seguinte forma: um colaborador preenche o formulário, com as todas as especificações técnicas, realizando o envio do formulário, assim gerando um ID, esse ID, vai para uma fila de requisições, como apresentado na Figura 5, posteriormente, utilizando *templates* desenvolvidos em Ansible, realiza-se o acesso a fila, selecionando o ultimo ID e o acessando para visualizar todas as informações contidas, definindo variáveis e realizando o direcionamento para *worflows* de trabalho para tarefa específica, como:

- Criar servidor virtual Windows;
- Criar servidor virtual Linux;
- Clone de servidor virtual Windows;
- Clone de servidor virtual Linux.

Figura 5 – Processo de requisição



Autor: Autoria própria

Ao longo da execução do *workflow*, realiza-se o envio de comentários a plataforma Service Now, com as etapas que estão sendo concluídas e ao final do workflow, realizando o fechamento dessa requisição, posteriormente, ocorre o envio de requisições para equipes técnicas para atualização de dados no sistema de monitoramento e inventário. O envio de comentários é importante, pois, para uma eventual falha na automação, irá auxiliar a equipe de servidores a compreender em momento ocorreu a falha e compreender o que ainda precisa ser feito nessa máquina.

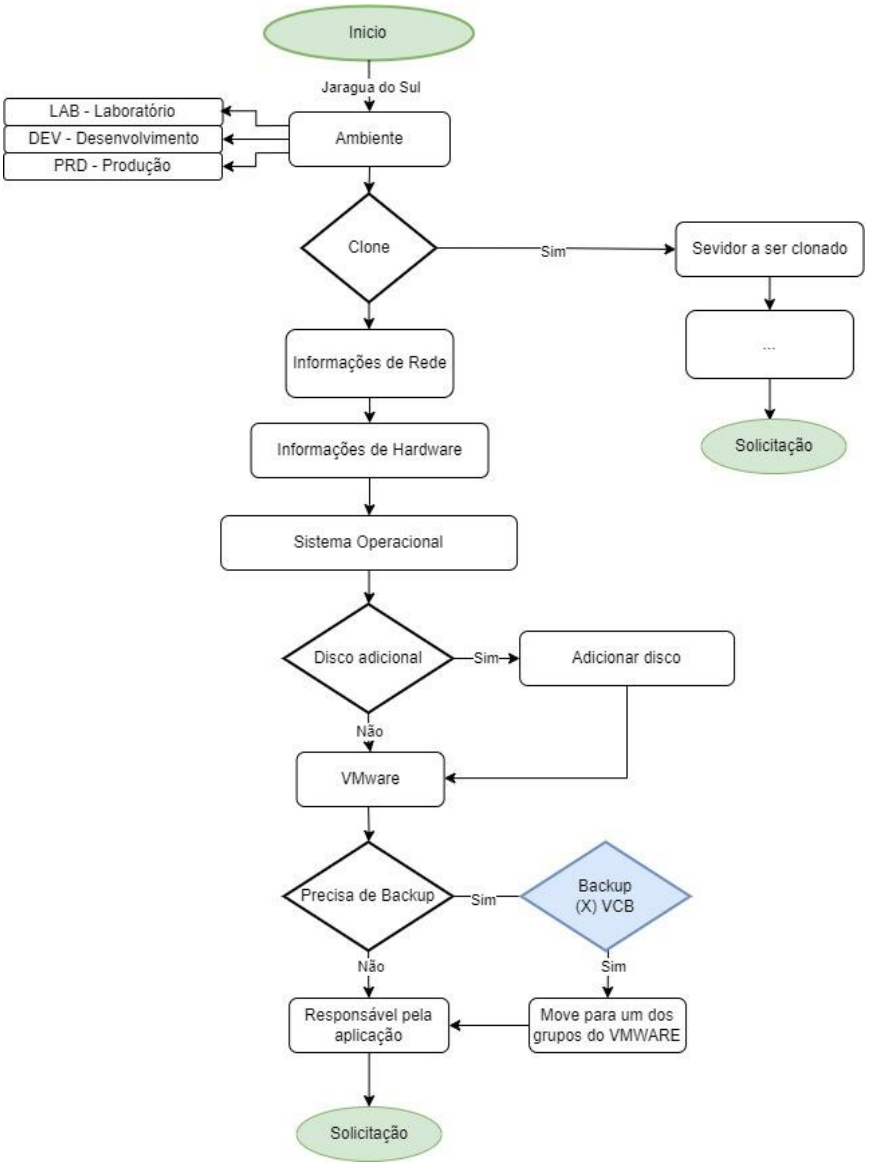
Formulário

O formulário em produção carecia de melhorias e parametrizações para bem de funcionar corretamente, o desenvolvimento de um fluxograma com filtros, ao qual corrigiu inconsistências no formulário anterior, como: escopo de opções aberto, ao qual permitia o colaborador preencher errado, informações erradas nos campos, campos escondidos, parametrização de exceções.

Dessa forma, foi realizado o desenvolvimento de um formulário do zero, ao qual desenvolvi o fluxograma, definindo com a equipe como precisaria ser, quais eram campos relevantes, filtros nas opções, assim, fechando o escopo conforme o colaborador preenche o formulário. Uma amostra no formulário pode ser vista na Figura 6, apresentando as principais informações a serem preenchidas, bem como sua estrutura.

Com o fluxograma desenvolvido, a equipe responsável pela Service Now, usou como referência no desenvolvimento do novo formulário. Em consorcio da equipe de servidores com a equipe do Service Now, foi definido uma estrutura de filas, ao qual cada requisição é armazenada por ordem de chegada e a qual, é usada para coletar o ID das requisições, bem como para acessar o conteúdo desta requisição.

Figura 6 – Fluxograma do formulário desenvolvido

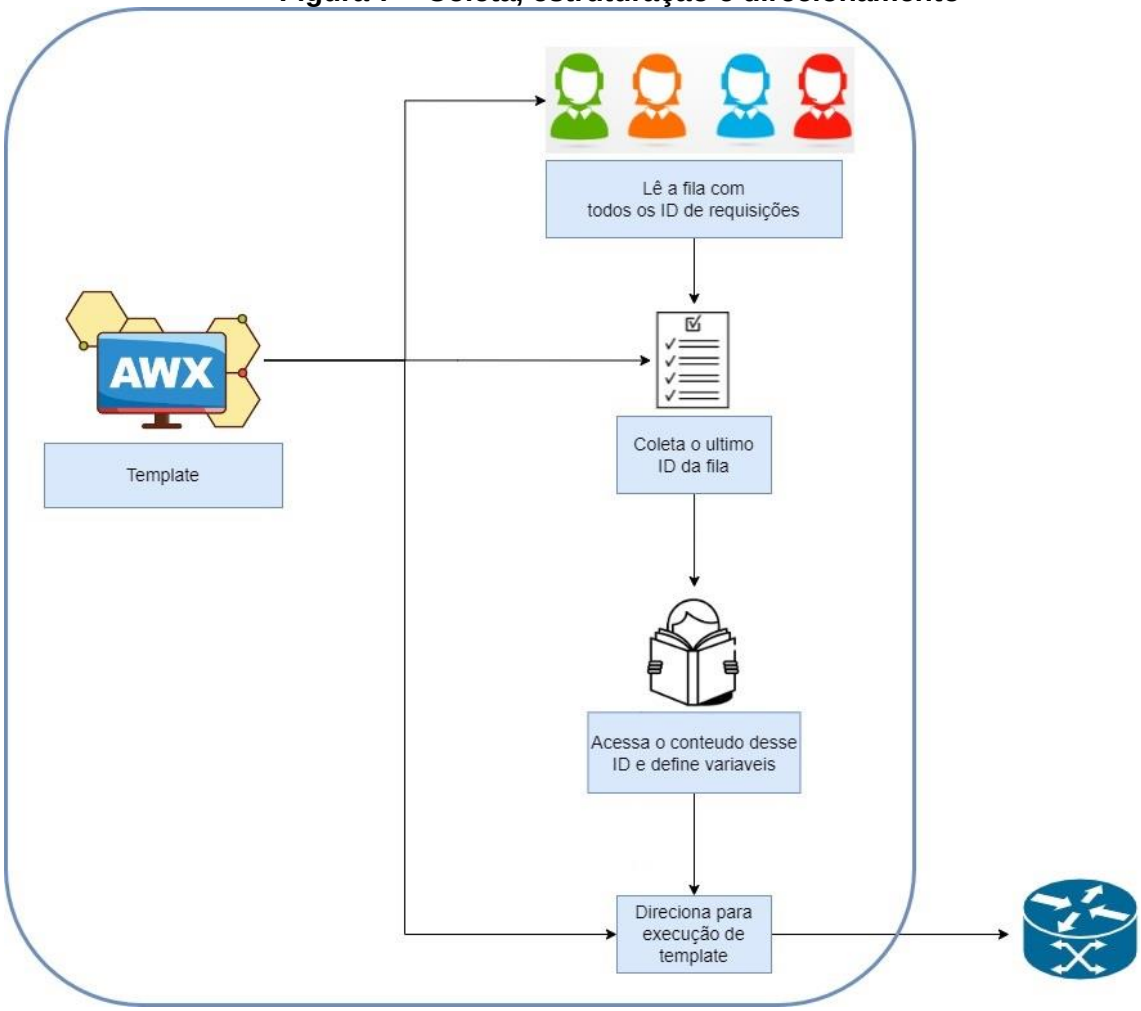


Autor: Autoria própria

Coleta, estruturação e direcionando

A etapa de coleta de dados, ocorre via integração de plataformas, utilizando a API do Service Now, por meio de *templates* Ansible, realizando a leitura da fila de chamados, coletando um ID, explorando o conteúdo do ID, coletando os dados, padronizando, definindo variáveis, assim, realizando o direcionamento para o *workflow* relacionado, realiza-se essas tarefas utilizando módulos Ansible e comandos Bash, tendo a plataforma AWX, como orquestradora das tarefas, conforme, representado na Figura 7.

Figura 7 – Coleta, estruturação e direcionamento

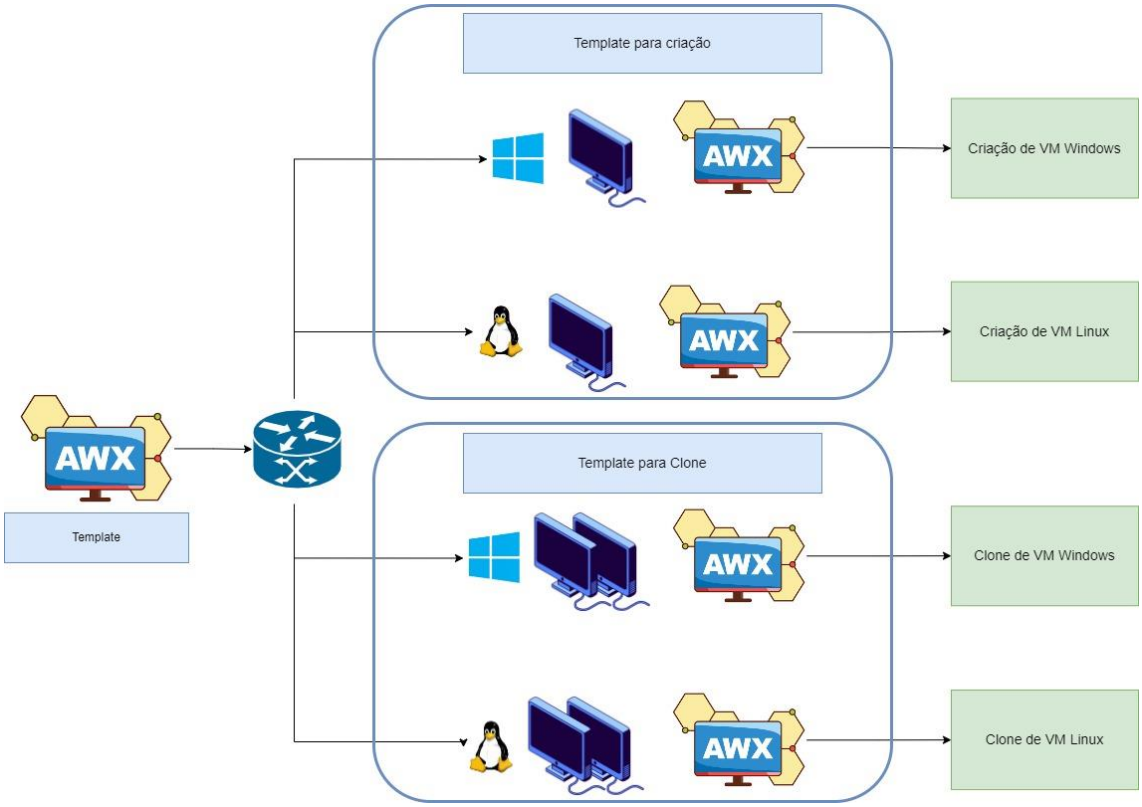


Autor: Autoria própria

Criação/Clone de Servidor Virtual

Na etapa de criação/clone, são realizadas, várias rotinas, como: cadastrar a máquina no VMware, *ActiveDiretory*, cadastro da senha do administrador no cofre de senhas, instalação de antivírus, formatação de discos e inicialização dos novos, ajustar para o horário de Brasília, inicializar serviços, entre outras tarefas, a Figura 8, apresenta o *workflow* a ser executado, conforme definido na etapa anterior com base nos dados contidos na requisição, assim direcionando a execução de tarefas.

Figura 8 – *Workflow*



Autor: Autoria própria

Ganhos

Os principais ganhos com a implantação dessa automação para a equipe de servidores, destacados por Anderson Mekelburg, estão:

- Padronização do processo de criação dos servidores virtuais;
- Ganho operacional reduzindo horas de trabalho de técnicos e analistas;
- Acuracidade das informações.

5.12 Descoberta automática da topologia Cisco

O processo de descoberta automática da topologia Cisco, busca realizar uma coleta de dados da topologia ao qual um switch está conectado, tendo como foco, modelos *Catalyst* da Cisco, esse *script*, busca realizar uma varredura rápida da rede, e será muito útil para reconhecer o cenário de filiais não integradas a domínio, também para compreender a topologia de unidades em processo de aquisição de filiais.

Desenvolvido em Python, seu funcionamento se dá da seguinte forma: o usuário informar um switch inicial e suas credenciais de login, o script busca conhecer os seus vizinhos, realizando o comando “*show cdp neighbors*” na console do switch, assim, coletando as informações de seus vizinhos, utiliza-se como parâmetro para reconhecer um switch seu padrão de *hostname*, com isso, cada vez o *script* se aprofundando mais na rede, a fim de conhecer todos e marcando os switches conhecidos para não se conectar novamente, assim montando a topologia de rede.

Os dados são organizados de maneira hierárquica, para isso, foi utilizado o conceito de estrutura de dados: árvores b, para construção da topologia, a qual, de um nó raiz, temos as folhas e dessas folhas, caso o dispositivo seja um switch e tenha vizinhos, essa folha se torna uma subarvore, aumentando o nível de profundidade da rede.

Exemplo de como o resultado está estruturado:

SWITCH001
- Gi1/0, SWITCH002
  - Gi2/0/2, ACESS_POINT001
  - Gi2/0/32, ACESS_POINT005
- Gi1/24, ACESS_POINT002
- Gi1/23, ACESS_POINT003
- Gi2/0/32, SWITCH003
  - Gi2/0/14, SWITCH0014
  - Gi2/0/14, SWITCH0027
    - Gi1/13, ACESS_POINT010
    - Gi1/15, ACESS_POINT012

O exemplo apresentado, o switch raiz informando é: SWITCH001, e possui como vizinhos: SWITCH002, ACESS_POINT002, ACESS_POINT003, SWITCH003, sendo assim, está conectado a dois *access point* e a dois switches que foram descobertos no primeiro dispositivo, que posteriormente o sistema irá percorrer esses dispositivos coletando informações.

5.13 Contagem de Mac Address

O script de contagem de *mac address* em switches, desenvolvido em Ansible, funcionou durante um mês, realizando coletas de dados por hora, o objetivo, foi compreender os horários de picos de *mac's* conectados e quantos mac existem conectados na rede.

Em seu funcionamento, realiza-se uma conexão ssh no switch, realizando um comando *“sh mac address-table count | in Dynamic*” na console, com o output comando, coletamos a quantidade de *mac address* no switch.

5.14 Backup de configuração

O *script* de *backup* de configuração, buscou realizar o *backup* de switches de maneira escalável e rápida, ao qual pode ser usado para diversas situações, como: consolidado das configurações do switch, estruturação de topologia, *backup* das configurações antes de realizar novas configurações, reconhecimento de novos cenários.

5.15 Informações das portas dos switches

O script buscou coletar uma série de informações sobre as portas dos switches, como: quantos *devices* conectados na porta, em qual *vlan* estão conectados, se tem erros naquela porta e se tem tráfego, sendo usado para reconhecer o ambiente (no caso, executar em uma rede nova), capturar informações para resolução de problemas (executar várias vezes e acompanhar as mudanças na porta - erros, tráfego etc.).

6 CONSIDERAÇÕES FINAIS

Considerando os fatos mencionados neste relatório, é evidente a relevância do estágio, pois ele coloca o estagiário no contexto do mercado de trabalho. As experiências adquiridas vão além das habilidades técnicas aprimoradas através do desenvolvimento das atividades no estágio, incluindo também as relações interpessoais no ambiente de trabalho. Houve um aumento significativo nos conhecimentos técnicos, principalmente relacionados a redes industriais, servidores, análise de dados, metodologias ágeis, além da melhoria na habilidade de comunicação interpessoal e trabalho em equipe. Como resultado deste estágio, para o âmbito de redes: foi possível compreender as aplicações que dominam o volume de dados trafegados, bem como os hosts com desvios de consumo em relação à norma, desenvolvendo soluções que são usadas no dia a dia. Isso irá auxiliar a equipe de projetos na tomada de decisão para o desenvolvimento e compreensão da arquitetura de novas filiais; no âmbito de servidores: a continuação, desenvolvimento e implantação de uma automação de criação/clone de servidores virtuais, tão almejada pela seção de sustentação, trazendo assim, ganho para todo Departamento de Infraestrutura. Dessa forma, destaco que o período de estágio na companhia, em especial o Departamento de Infraestrutura, atuando diretamente nas seções de Projetos e Sustentação, foi um período de intenso aprendizado, muitas melhorias como profissional, atuando em projetos de impacto no dia a dia, desenvolvendo soluções que iram impactar positivamente o dia a dia da equipe, assim estando grato a toda equipe do Departamento de Infraestrutura, pela acolhida e a oportunidade de desenvolvimento durante o período de estágio, especialmente aos meus padrinhos: Andrei Goncalvez e Anderson Mekelburg, que estiveram me auxiliando e acompanhando diretamente a realização de tarefas.

REFERÊNCIAS

KENTIK. What is Network Observability? Disponível em: https://www.kentik.com/kentipedia/what-is-network-observability. Acesso em: 9 mar. 2023.

WILLIAM, H. 10 Network Monitoring Best Practices You Need to Know About. Disponível em: https://www.insightsforprofessionals.com/it/network/network-monitoring-best-practices. Acesso em: 9 mar. 2023.

POSITIVO T. Como melhorar a qualidade dos serviços de aplicações. Disponível em: https://www.meupositivo.com.br/panoramapositivo/observability/. Acesso em: 9 mar. 2023.

LAMBERTI, Alyssa. 19 Network Metrics: How to Measure Network Performance. Obkio, 6 mar. 2023. Available at: https://obkio.com/blog/how-to-measure-network-performance-metrics/. Acessado em: 16 ago. 2023.

WEG. WEG. Disponível em: https://www.weg.net/institutional/BR/pt/. Acesso em: 14 ago. 2023.

ALURA. Formação Redes. Disponível em: https://www.alura.com.br/formacao-redes. Acesso em: 14 ago. 2023.

PHOENIXNAP. O que é SNMP? Disponível em: https://phoenixnap.com/kb/what-is-snmp. Acesso em: 14 ago. 2023.

SOLARWINDS. NetFlow Traffic Analyzer. Disponível em: https://www.solarwinds.com/pt/netflow-traffic-analyzer. Acesso em: 14 ago. 2023.

VMWARE. Virtualização de servidores. Disponível em: https://www.vmware.com/br/topics/glossary/content/server-virtualization.html. Acesso em: 14 dez. 2023.

REDHAT. Logical Volume Manager Administration. Disponível em: https://access.redhat.com/documentation/pt-br/red_hat_enterprise_linux/6/html/logical_volume_manager_administration/index. Acesso em: 14 dez. 2023.