Igor Henrique Sousa de Andrade

SysOps Senior at HostGator

Rua Tertuliano de Castro, N° 1287, Bessa, João Pessoa – PB Solteiro, 34 anos
Telefone: (83) 999650-2851 / E-mail: igor@igorlnx.com
Linkedin: https://www.linkedin.com/in/igor-andrade-244221160/
Github https://github.com/igorhrq
Gist GitHub: https://gist.github.com/igorhrq
Site: https://igorlnx.com (Apenas em inglês)
Mantenedor do blog: https://debian-pb.org (Grupo de Usuários Debian da Paraíba)

CERTIFICAÇÕES

LPIC-1 – Ver aqui
Comptia Linux+ - Visualizar aqui
Plesk Onyx Professional - https://igorlnx.com/plesk-igorandrade.pdf
NSE 1 Network Security Associate (FORTINET) – https://igorlnx.com/NSE_1_Certificate.pdf
NSE 2 Network Security Associate (FORTINET) - https://igorlnx.com/NSE_2_Certificate.pdf
DevOps Essentials Professional by Certiprof – Download PDF
Scrum Foundation Professional by Certiprof – Download PDF
Imunify360 by cPanel University – Download Certificate
cPanel Professional Certification (CPP) - http://igorlnx.com/CWAandCPP.png
cPanel & WHM Administrator Certification (CWA) - http://igorlnx.com/CWAandCPP.png
KanBan Foundation Certificate (KIKF) ™ - http://igorlnx.com/kanban.pdf
Cyber Security Foundation – CSFPC - https://igorlnx.com/certs/CSFPC.pdf
GitLab Certified Associate – Link to certificate

FORMAÇÃO ACADÊMICA

Pós-Graduação em Segurança da informação - Unipê

Pós-Graduação em segurança da informação: 2016 - 2017 (Incompleto)

Redes de Computadores – Estácio

Curso superior em Redes de Computadores na Estácio de Sá da Paraíba: 2013 – 2016 (Completo)

ÁREAS DE INTERESSE

- **Observabilidade**
  - APM's como DataDog, NewRelic
  - Entrega Amigável com Grafana e também alertas via webhook
  - Zabbix para infraestrutura
  - Graylog para logs (solução OpenSource)

- **Segurança da informação**
  - Análise de Vulnerabilidade
  - Obfuscation
  - OS Hardening, Solutions Hardening
  - Auditing
- **DevOps**
  - IaC
  - Aplicação de patchs em massa e configurações em massa e persistência
- **Linux Administration**
  - Shell Scripting
  - Python

Profissional

- *Abril 2022 – Atualmente* **HostGator LatAm / NewFold Digital**

Site: https://newfold.com/

Cargo: SysOps Senior

- ***Observability:*** *Plano de Observabilidade com Datadog, onde serviços criticos eram monitorados com Synthetics tests, Browser tests, SSL Tests, Dashboards, análise de querys via Ferramenta (DPM), criando assim triggers para disparar em canais do time, integração do cloudwatch com o Datadog, criando o lambda para coleta dos logs dos serviços/microservices na AWS;*
- ***Observability:*** *Criação de scripts em python para consumir API ou criar API com flask e assim exibir um json com status de diversos serviços necessários em formato Healthcheck*
- ***Observability:*** *Integração Zabbix e Teams com um script em python, todos alertas criticos do core eram disparados em nossa sala, separando apenas para o grupo core*
- ***Observability:*** *Trabalho intensivo com Grafana, trazendo a cultura de observabilidade. Criei uma dashboard onde todo fluxo de pagamento da HostGator era monitorado, desde a geração de um simples boleto, até como um sistema que monitorava clientes com saldos elevados, além de exibir de forma amigável no grafana, disparava alertas críticos.*
- ***Observability:*** *Criação de vários scripts pontuais em Python e bash para certos tipos de demandas, para monitorias especificas e de baixa criticidade ou de solicitações de times próximos*
- ***Observability:*** *Integração Zabbix + Grafana, para monitorar recursos disponíveis das maquinas cores, criando uma dashboard para monitoramento.*
- ***Migrações Complexas:*** *Remoção de diversos pontos de falha da infraestrutura Billing LatAm, migrando para um ambiente completamente redundante com HAProxy e Galera Cluster, com redundância de 2 nodes para Haproxy/webservice/PostFix e 3 nodes para o Percona XtraDB Cluster.*
- ***Migrações Complexas:*** *Migração de ambientes do time do Business Inteligence LatAm, com soluções como Pentaho, Qlik, Postgres, hadoop e outras*
- ***DevOps:*** *Execução em massa via ansible para configuração de serviço, atualização de certificados ou aplicação de patchs/update(geralmente segurança) dentro dos 5 nodes do ambiente Billing Brasil e Billing LatAm(colombia, mexico e chile)*
- ***DevOps:*** *Atualização de certificados de ambientes compartilhados de hospedagem via Puppet, bem como novas configurações*
- *Manutenção do servidor de e-mail core (Garantir entrega, reputação etc)*
- *Identificar qualquer incidente que esteja relacionado a pagamentos bem como correção, caso contrário acionar setores responsáveis, se a correção não for a nível de sistema;*

- *Estudo de novas soluções, desenho e melhorarias de soluções atuais quando necessário, consequentemente implementar para produção;*
- *Implementação de soluções de segurança com CloudFlare, além de integração com Grafana*
- *Integração Azure AD + Grafana, todos os usuários do Azure AD foram integrados como oAUTH do grafana, assim reduzimos riscos de segurança e centralizamos os logins, desativei meio local.*

- *Novembro 2020 – Março 2022* **HostGator LatAm / NewFold Digital**

Site: https://newfold.com/

Cargo: SysOps Pleno

- Manter ambiente core da HostGator LatAm(Empresa do grupo NewFold) Atualizado, seguro e estável;
- Administrar monitoramento atual para melhor eficácia assim como melhorias no mesmo;
- Identificar qualquer incidente que esteja relacionado a pagamentos bem como correção, caso contrário acionar setores responsáveis, se a correção não for a nível de sistema;
- Criação de scripts Python e Shell para melhorias do ambiente core;
- Criação de dashboards no grafana + zabbix para monitorar recursos das máquinas cores e também todo sistema de pagamento usado na empresa
- Garantir backups atualizados para se necessário, utilizado;
- Estudo de novas soluções, desenho e melhorarias de soluções atuais quando necessário, consequentemente implementar para produção;
- Filtrar e resolver os problemas a partir de sua complexidade;
- Aplicar patchs de atualização a nível de sistema
- Manutenção do servidor de e-mail core (Garantir entrega, reputação etc)
- Execução em massa via ansible para configuração ou aplicação de patchs/update

- *Janeiro 2019 – Novembro 2020* **HostDime Brasil**

Site: https://hostdime.com.br

Cargo: Analista de Segurança Júnior

- Interação direta com o cliente através dos canais de atendimento (Ticket);
- Filtrar e resolver os problemas a partir de sua complexidade;
- Suporte Avançado em Soluções Personalizadas (Zimbra Mail, xcp-ng/xen, Docker, pfsense, lemp/lamp, open-vpn e fortigate)
- Migrações de alta complexidade (cPanel, E-mails, s/ painel, etc)
- Desenvolvimento de Scripts Shell/Bash para automatizar tarefas complexas e atacar demandas pertinentes: meu gist.github.com
- Aplicar Patchs de atualização em massa com Ansible/WinRM ou via WSUS(Windows)
- Estudo de novas soluções para trazer melhorias e atacar certas demandas que eventualmente possa escoar um problema frequente
- Planejamento de Capacidade em Ambientes Linux ou Windows para ofertar upgrades para clientes que possuam gargalos com o hardware/recurso atual.
- Criação de Políticas via Confluence(Knowledge Base) focadas na segurança de todos os ambientes/setores/soluções da Empresa tanto de clientes como soluções internas, enumerando todas as eventuais brechas/gaps e correção das mesmas conscientizando todos os colaboradores.
- Análise de Vulnerabilidades em sistemas internos com (Nessus, Qualys, nikto, arachni e nmap)
- Monitoramento com Zabbix para identificar vários comportamentos e se antecipar a problemas com os clientes (partição cheia, fila de e-mails alta, versões de softwares desatualizados e etc)

- *Março 2018 – Dezembro 2018* **HostDime Brasil**

Site: https://hostdime.com.br

Cargo: SysOps

- Administração Avançada de ambientes Linux e Windows c/ ou s/ Painel Plesk/cPanel/CWP/LEMP/LAMP e seus respectivos serviços
- Interação direta com o cliente através dos canais de atendimento (Ticket);
- Filtrar e resolver os problemas a partir de sua complexidade;

- Suporte Avançado em Soluções Personalizadas (Zimbra Mail, xcp-ng/xen, Docker, pfsense, lemp/lamp, open-vpn e fortigate)
- Migrações de alta complexidade (cPanel, E-mails, s/ painel, etc)
- Desenvolvimento de Scripts Shell/Bash para automatizar tarefas complexas e atacar demandas pertinentes: meu gist.github.com
- Aplicar Patchs de atualização em massa com Ansible/WinRM ou via WSUS(Windows)
- Estudo de novas soluções para trazer melhorias e atacar certas demandas que eventualmente possa escoar um problema frequente
- Planejamento de Capacidade em Ambientes Linux ou Windows para ofertar upgrades para clientes que possuam gargalos com o hardware/recurso atual.
- Monitor (Windows) para ver spikes e uso de tráfego excessivo
- Auditoria de Tráfego Outbound/Inbound com nload/iptraf/netstat/lsof/cacti/zabbix ou Network

Janeiro de 2016 – Janeiro 2018 **HostDime Brasil**

Site: https://www.hostdime.com.br

Cargo: Analista de Suporte Level II e III

- Administração Avançada de ambientes Linux e Windows c/ ou s/ Painel Plesk/cPanel/CWP/LEMP/LAMP e seus respectivos serviços
- Interação direta com o cliente através dos canais de atendimento (Ticket);
- Filtrar e resolver os problemas a partir de sua complexidade;
- Auditoria Intermediária em contas cPanel/Plesk ou s/ painel Identificação e Mitigação de abusos (Comprometimento de complexidade média geralmente ocorrido via aplicação (outdated) e de contas de e-mails na máquina remota ou script)
- Suporte em Soluções Personalizadas (Zimbra Mail, xcp-ng/xen, pfsense, lemp/lamp, open-vpn e fortigate)
- Desenvolvimento de Scripts Shell/Bash/Python para automatizar tarefas e atacar demandas pertinentes: meu gist.github.com

- *Abril 2015 – Janeiro 2016* **HostDime Brasil**

Site: https://www.hostdime.com.br

Cargo: Analista de Suporte Level I

- Administração Intermediária de ambientes Linux e Windows c/ ou s/ Painel Plesk/cPanel/CWP/LEMP/LAMP e seus respectivos serviços
- Auditoria Avançada em contas cPanel/Plesk ou s/ painel, Identificação e Mitigação de abusos (Comprometimento de complexidade Alta geralmente ocorrido via aplicação (outdated) e de contas de emails na máquina remota ou script, identificação e mitigação de ataques brute-force, criação de regras modsecurity se necessário ou ajustes a nível de firewall iptables/csf)

- Interação direta com o cliente através dos canais de atendimento (Telefone, Chat e Ticket);
- Filtrar e resolver os problemas a partir de sua complexidade;
- Elaboração de artigos e tutoriais internos e públicos para auxiliar os clientes. (ajuda.hostdime.com.br)
- Auditoria Básica em contas cPanel (Identificação e mitigação de SPAM de comprometimentos de baixa complexidade)

- *Janeiro 2015 – Abril 2015* **HostDime Brasil**

Site: https://www.hostdime.com.br

Cargo: Estagiário de Suporte

- Administração básica de ambientes Linux e Windows c/ ou s/ Painel Plesk/cPanel/CWP e seus respectivos serviços
- Interação direta com o cliente através dos canais de atendimento (Telefone, Chat e Ticket);
- Filtrar e resolver os problemas a partir de sua complexidade;
- Elaboração de artigos e tutoriais internos e públicos para auxiliar os clientes. (ajuda.hostdime.com.br)

HABILIDADES

- Linux Administration & Hardening;
- Apache, nginx, exim, postfix, varnish cache, imapsync
- HAProxy (Cluster de alta disponibilidade com fácil escalabilidade)
- KVM, Proxmox, XCP-Ng(Virtualização)
- Docker e OpenVZ; (Container)
- Datadog e Graylog (Pilha Observability)
- Zabbix and Grafana (Pilha Observability)
- Bash/Shell Script/Regex;
- Python (Criação de APIs com flask + consumir APIs e scripts)
- Zimbra Mail;
- wpscan, nmap, sqlmap, metasploit, clamav + yara rules, modsecurity, arachni, nessus, qualys, deepsecurity, owasp zap (Pilha infosec)
- iptables, csf, pfsense, endian(iptables), fortigate; (Pilha infosec)
- AWS (ec2/s3/cloudwatch/cloudformation/route53/lambda)
- git, gitlab and github;
- Ferramentas Atlassian(JIRA, confluence, bitbucket and bamboo);
- MySQL, MariaDB, PostgreSQL, PerconaDB
- Galera Cluster (PerconaXtraDB Cluster) (Cluster MySQL de alta disponibilidade)
- Bacula (Gerencia de backups)
- CloudFlare (Ferramentas de segurança/Observability e integração de Plugin com Grafana)
- cPanel, Plesk, CWP, Imunify360, MagicSPAM, ClamAV, cpnginx, engintron, litespeed

IDIOMAS

- Inglês Fluente
- Espanhol Intermediário

CURSOS COMPLEMENTARES

- Pen Test: Técnicas de Intrusão em Redes Corporativas - Certificado
- Python para Iniciantes - Certificado
- Ferramentas de Automação DevOps Ansible, Chef e Puppet - Certificado
- Docker – Introdução a administração de Containers – Certificado
- Proxmox (Gerencia de Máquinas virtuais com Proxmox) - Certificado