**Monitoramento de Rede:** o monitoramento de rede monitorará e rastreará tudo sobre a rede. É um processo crítico em qualquer ambiente DevOps. O Monitoramento de Rede monitorará componentes de rede como roteadores, firewalls, servidores, switches e VMs. Em geral, os sistemas de Monitoramento de Rede (NMS) compartilham cinco pontos de dados críticos:

•Descobrir

•Mapear

•Monitorar

•Alertar

•Relatar

**DevOps:** DevOps é uma cultura, conjunto de práticas e ferramentas que visa a colaboração e integração entre as equipes de desenvolvimento (Dev) e operações (Ops) de software, buscando acelerar a entrega de valor aos clientes. O objetivo é quebrar silos entre as equipes, promovendo a automação de processos e a comunicação constante para otimizar o ciclo de vida do desenvolvimento e da entrega do software.

**Silos:** Equilibrar silos entre equipes significa encontrar um ponto de equilíbrio na organização onde diferentes departamentos ou equipes cooperam e compartilham informações, evitando o isolamento e a falta de comunicação que caracterizam os "silos" organizacionais. O objetivo é promover a colaboração, a eficiência e a troca de conhecimento entre as equipes, ao invés de cada uma trabalhar de forma isolada, como em silos separados.

**Monitoramento contínuo em DevOps:** Adotando DevOps para as empresas, geram respostas mais rápidas às necessidades dos clientes incluindo a entrega e implementações continuas. Muitas vezes em DevOps monitoramento continuo é negligenciado, essa pratica garante que os sistemas de entrega e implementação sejam monitorados gerando segurança ao longo do ciclo de vida das operações de TI.

**ConMon:** Significa Monitoramento Contínuo, crucial para rastrear e resolver problemas em tempo real, fornecendo feedback às equipes de desenvolvimento e operações (DevOps). Essa pratica além de eliminar silos entre as equipes, permite que identifiquem partes da aplicação que precisam de melhorias, sendo rapidamente detectado e tratado.

**Tipos de monitoramento no DevOps**

**Monitoramento de Infraestrutura:** Analisa servidores e redes.

Algumas das ferramentas populares de Monitoramento de Infraestrutura incluem Nagios, Zabbix, ManageEngine OpManager, SolarWinds, Prometheus, etc.

**Monitoramento de Aplicações:** Avalia o desempenho e a segurança das aplicações.

Algumas das ferramentas APM populares são AppDynamics, Dynatrace, Datadog, Uptime Robot, Uptrends, Splunk, etc.

**Monitoramento de Rede:** Rastreia componentes como roteadores e firewalls.

Algumas das ferramentas NMS populares incluem Cacti, ntop, nmap, Spiceworks, Wireshark, Traceroute, Bandwidth Monitor, etc.

Cada tipo é essencial para garantir a eficiência e a disponibilidade dos serviços oferecidos pela organização.

**Ferramentas de monitoramento em 2020:** São fundamentais para o sucesso do DevOps, as principais ferramentas são: Nagios, Monit, Consul, Datadog, Prometheus, PagerDuty, Snort e Splunk. Cada ferramenta oferece uma funcionalidade especifica como monitoramento de infraestrutura, alertas e analises em tempo real de dados, além de garantir a segurança também mantem a performance dos sistemas.

**Relevância das Ferramentas de Monitoramento:** São vitais para a eficiência do DevOps, ajudam em várias áreas como detectar problemas rapidamente, melhorando a colaboração entre as equipes e garantido que os serviços estejam sempre disponíveis. É essencial a escolha da ferramenta certa pois pode impactar diretamente a qualidade e a segurança das aplicações, tornando o ConMon uma prioridade em Ti.

**Melhores Ferramentas de Monitoramento DevOps em 2020**

**1.Nagios: Nagios é uma ferramenta de monitoramento DevOps de código aberto. Ela ajudará o DevOps a encontrar e corrigir problemas com rede e infraestrutura. Recursos:**

•Simplifica o processo de busca de dados de log.

•Fornece monitoramento completo de sistemas operacionais de desktop e servidor.

•A ferramenta de gerenciamento de logs é líder na indústria.

•Fornece monitoramento completo de Java Management Extensions.

**2.Monit: Monit é uma ferramenta de monitoramento DevOps de código aberto. O Monit é projetado especialmente para monitorar sistemas operacionais UNIX. Recursos:**

•Realiza manutenção e reparo automáticos.

•Executa ações significativas em situações de erro.

•Ajuda a monitorar arquivos, diretórios e arquivos no localhost.

•Permite conexões de rede a diferentes servidores.

**3.Consul: Consul é outra ferramenta de monitoramento de código aberto (pertencente à HashiCorp). O Consul é usado para descobrir e configurar serviços em qualquer infraestrutura. Recursos:**

•A ferramenta perfeita para infraestrutura moderna.

•Fornece uma API robusta.

•Fácil de encontrar serviços que cada aplicativo precisa usando DNS ou HTTP.

•Suporta múltiplos data centers.

**4.Datadog: Datadog é um serviço de monitoramento pago, que fornece monitoramento de servidores, aplicativos, bancos de dados, ferramentas e serviços através de uma plataforma SaaS inteligente. Recursos:**

•Painéis de monitoramento facilmente personalizáveis.

•Mais de 80 integrações prontas.

•Acesso completo às APIs.

•Obtenha visibilidade na saúde e desempenho das ferramentas DevOps.

•Visualize dados de sistemas upstream e downstream com métricas, rastreamentos e logs.

**5.Prometheus: solução de monitoramento de código aberto, construída principalmente para coletar e analisar dados de séries temporais. Ele usa SNMP para coletar dados de desempenho de dispositivos na rede. Recursos:**

•O Prometheus coleta dados ativamente, armazena e suporta consultas, gráficos e alertas.

•Reduz o tempo de configuração do ambiente de desenvolvimento.

•Funciona perfeitamente com Mac, Windows e Linux.

•Muito popular para monitorar ambientes conteinerizados (Docker, Kubernetes).

•Integra-se com ferramentas de configuração existentes como Chef, Puppet, Ansible, Salt.

•Cria um único arquivo para projetos descreverem que tipo de máquina e software os usuários desejam instalar.

**6.PagerDuty: PagerDuty é uma ferramenta de alerta paga. Ela ajuda as empresas a melhorar a reputação de sua marca. O PagerDuty permite que a equipe DevOps entregue aplicativos de alto desempenho. Recursos:**

•Coleta de dados via um modelo de pull sobre HTTP.

•Suporta múltiplos modos para gráficos e painéis.

•Funciona como nós de servidor autônomos sem dependência de armazenamento distribuído.

**7.Snort: Snort é um sistema de detecção de intrusões em rede (NIDS) de código aberto. Snort é uma ferramenta poderosa que ajuda a detectar intrusos na rede. Recursos:**

•Permite análise de tráfego em tempo real e registro de pacotes.

•Realiza análise de protocolo e busca de conteúdo.

•Detecta estouros de buffer, varreduras de portas furtivas e tentativas de identificação de sistema operacional.

**8.Splunk: Splunk é uma ferramenta paga. Ela torna os dados de máquina acessíveis e utilizáveis para todos. É uma plataforma de software para buscar, analisar e visualizar os dados gerados por máquinas coletados de todos os componentes da infraestrutura de TI. Recursos:**

•Fornece inteligência operacional para a equipe DevOps.

•Análise orientada por dados com insights acionáveis.

•Oferece uma visão única e unificada de vários serviços de TI.

•Você pode estender a plataforma Splunk com soluções específicas para segurança.