



UNIVERSIDADE CATÓLICA DE PELOTAS
ENGENHARIA DE COMPUTAÇÃO
Redes de computadores

Gabriel Harter Zoppo

Nagios Core - Visão Geral

Pelotas,
15/10/2021

1. O que é o Nagios Core:

Nagios Core é o sistema de monitoramento Open Source que permite às organizações identificar e resolver problemas de infraestrutura de TI antes que eles afetem os processos críticos de negócios.

O Nagios Core serve como um dos blocos de desenvolvimento do Nagios XI que é a solução de monitoramento comercial.

Nagios Core permite que você monitore toda a sua infraestrutura de TI para garantir que os sistemas, aplicativos, serviços e processos de negócios estão funcionando corretamente. No caso de uma falha, ele pode alertar os responsáveis técnicos do problema, permitindo-lhes começar o processo de correção antes que as interrupções afetem os processos de negócios, usuários finais ou clientes.

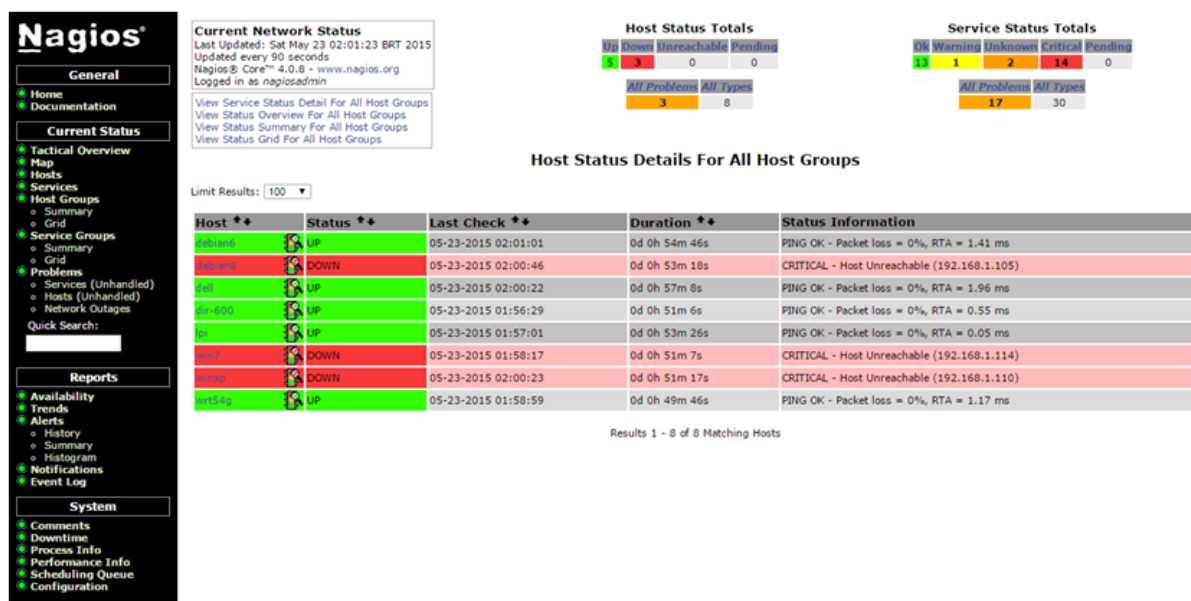


Figura 1: Interface do Nagios Core

2. Motivação para criação:

Nagios foi criado por um estudante de ciência da computação da universidade de Minnesota, no seu primeiro trabalho como administrador de redes, durante uma das reuniões da empresa um dos servidores parou de funcionar causando bastante problemas para todos da empresa. Diante dessa situação ele sentiu a necessidade de monitorar o sistema e saber se ele está funcionando ou não.

3. História do nagios:

1996: Ethan Galstad cria um aplicativo simples de MS-DOS projetado para “ping” servidores Novell Netware e enviar páginas numéricas. O aplicativo é projetado usando aplicativos externos de terceiros para realizar as verificações do servidor e enviar páginas. Nasce o conceito arquitetônico básico que será usado no Nagios.

1998: Considerando a possibilidade de entrar no negócio de monitoramento hospedado / serviços gerenciados, Ethan usa as idéias e a arquitetura de seu trabalho anterior para começar a construir um aplicativo novo e aprimorado projetado para rodar no Linux.

1999: Ethan lança seu trabalho como um projeto Open Source com o nome “NetSaint”. Ele estima que pode haver cerca de uma dúzia de outras pessoas que podem estar interessadas no aplicativo.

Os plug-ins que foram originalmente distribuídos como parte da distribuição NetSaint logo são desmembrados como um projeto separado de plugins do Nagios.

2002: Devido a problemas de marca registrada com o nome “NetSaint” que poderiam ter um impacto de longo prazo, Ethan decide renomear o projeto para “Nagios”, que era um acrônimo recursivo para “Nagios Ain't Gonna Insist On Sainthood”. O desenvolvimento do projeto NetSaint Plugins foi movido para o projeto Nagios Plugins.

2007: Ethan fundou a Nagios Enterprises, LLC para fornecer serviços de consultoria e desenvolvimento em Nagios.

2009: Os contratos de suporte anual são oficialmente oferecidos pela primeira vez pela Nagios Enterprises.

Nagios Enterprises lança seu primeiro produto de monitoramento comercial, Nagios XI.

Nagios foi renomeado para Nagios Core.

2010: O Nagios Fusion é lançado como um painel de servidor de monitoramento central.

2011: O Nagios BPI é lançado para monitorar processos de negócios.

2012: O NSTI foi lançado para gerenciar traps SNMP.

O Nagios Incident Manager é lançado.

2013: O Nagios Network Analyzer foi lançado para fornecer uma análise aprofundada dos padrões de tráfego da rede.

O NCPA foi lançado para fornecer um agente de monitoramento de plataforma cruzada extensível.

Nagios Core 4 é lançado.

2014: Nagios anuncia que a equipe do Nagios Plugin está passando por algumas mudanças, incluindo a introdução de um novo mantenedor.

O Nagios Log Server foi lançado para fornecer monitoramento e gerenciamento de log de classe empresarial.

2015: O Nagios XI 5 chega com mais de 200 aprimoramentos e melhorias.

4. Visão Geral da arquitetura:

Em algumas versões do Nagios, o usuário pode optar por trabalhar na interface de linha de comando (CLI) ou na interface gráfica do usuário (GUI) baseada na web de terceiros. O painel do Nagios fornece uma visão geral dos parâmetros críticos monitorados nos ativos.

Dependendo dos parâmetros e limites definidos, o Nagios pode enviar alertas quando níveis críticos são atingidos. Essas notificações podem ser enviadas de diferentes maneiras, incluindo e-mail e mensagens de texto. Com o sistema de autorização, o administrador tem permissão para restringir o acesso.

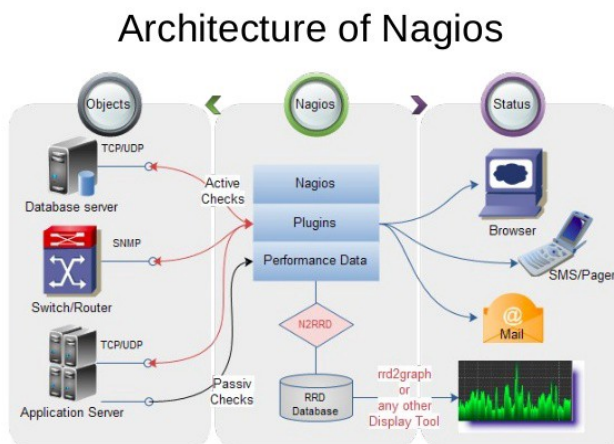


Figura 2: Arquitetura do Nagios.

O Nagios suporta add-ons que são add-ons e extensões autônomas, para que o usuário possa definir destinos e determinar quais parâmetros seguir nestes destinos. Os plugins do Nagios processam argumentos de linha de comando e passam comandos pelo Nagios Core. Esses plugins são categorizados em listas, incluindo hardware, software, nuvem, sistema operacional, segurança, arquivos de log e conexões de rede. Por exemplo, quando usado em conjunto com sistemas de detecção ambiental, um plug-in Nagios pode compartilhar dados sobre variáveis ambientais, como temperatura, umidade ou pressão barométrica.

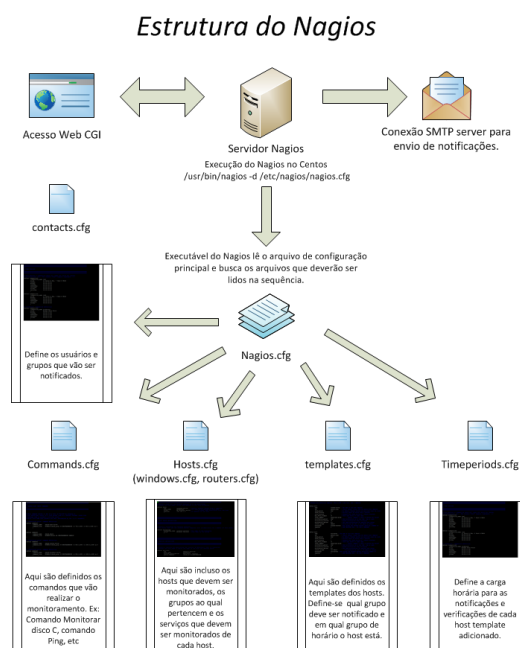


Figura 3: Estrutura do nagios

5. Funcionalidades:

Monitoramento: A equipe de TI configura o Nagios para monitorar componentes críticos da infraestrutura de TI, incluindo métricas de sistemas, protocolos de rede, aplicações, serviços, servidores e a infraestrutura de rede.

Alertas: O Nagios envia alertas quando componentes críticos de infraestrutura falham ou se recuperam, fornecendo aos administradores as notificações de eventos importantes. Os alertas podem ser entregues via email, SMS ou por um script personalizado como abertura de chamado em um sistema de gerenciamento de incidentes como o OTRS.

Resposta: A equipe de TI pode tomar conhecimento dos alertas e começar a solucionar as interrupções e investigar os alertas de segurança imediatamente. Esses alertas podem ser escalados em diferentes grupos solucionadores se não forem tratados em tempo hábil.

Relatórios: Os relatórios fornecem registros históricos das interrupções dos eventos notificados e da resposta aos alertas para acompanhamento futuro. O relatório de disponibilidade ajuda a garantir que as métricas de SLAs estão sendo cumpridas.

Manutenção: O agendamento de tempo de inatividade(downtime) previne o envio de alertas durante uma manutenção agendada como aplicação de windows update.

Planejamento: Os gráficos e relatórios de planejamento de tendências e de capacidade permitem identificar as atualizações de infraestrutura necessárias antes que ocorram falhas.

6. Como Instalar Nagios Core:

Abaixo temos um vídeo mostrando passo a passo como instalar e configurar o nagios core.

<https://www.youtube.com/watch?v=EZyInhzbnnU>