FACULDADE ALCIDES MAYA TECNOLOGIA– AMTEC
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

DEIVI ANDERSON SILVA DE OLIVEIRA

NAGIOS - UMA FORMA DE MONITORAMENTO E CONTROLE EM AMBIENTE EDUCACIONAL

Porto Alegre
2019

DEIVI ANDERSON SILVA DE OLIVEIRA

NAGIOS-UMA FORMA DE MONITORAMENTO E CONTROLE EM AMBIENTE EDUCACIONAL

Projeto de Pesquisa apresentado como requisito parcial para obtenção do título de Tecnólogoem Redes de Computadores, pelo Curso de Redes de Computadores da Faculdade de Tecnologia Alcides Maya - AMTEC

Orientador: Prof. Anderson

Porto Alegre

2019

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CGI	Common Gateway Interface
CPU	Central Processing Unit
DNS	Domain Name System
GNU	GNU'sNot Unix
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
JMX	Java Management Extensions
MIB	Management Information Base
NBR	Normas Brasileiras de Regulação
OS	Operation System – Sistema Operacional
PC	Personal Computer
PING	Packet InterNet Groper
RFC	Request for Comments
SNMP	Simple Network Management Protocol
SSH	Secure SHell – Shell Seguro
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
UDP	User Datagram Protocol
UPS	Uninterruptable Power Supply

SUMÁRIO

1 INTRODUÇÃO

As infraestruturas de uma rede de computadores crescem de maneira elevada, aumentando a necessidade de manutenção e monitoramento no ambiente educacional. As máquinas conectadas diariamente são motivos que levam o administrador da rede se preocupar, e o monitoramento constante dos ativos ligados na rede como servidores, serviços de rede e aplicações, precisam ser verificados para saber se estão com alguma falha.

Uma rede de computadores necessita de ferramentas de monitoramento para gerenciar e registrar problemas ocorridos, para que possam ser analisados para uma possível solução. Para isso podemos contar com a ferramenta Nagios, para um melhor controle na rede educacional sendo capaz de monitorar os ativos de redes ligados.

Ao realizar o trabalho proposto foram utilizados os seguintes itens: Criação de um cenário para um método experimental, simulando um ambiente educacional, composto por roteadores, switch, servidores, computadores e impressora, onde o sistema de monitoramento Nagios Core Versão 4.4.1instalado em um servidor, ficara centralizado com intuito de coletar informações dos ativos de rede e serviços para notificar possíveis erros que podem acontecer.

Para que o Servidor Nagios, consiga buscar as informações dos ativos de rede e serviços, será instalado um agente NSclient nos computadores e servidores buscando informações do espaço em disco, memória, CPU e a disponibilidades dos serviços se esta UP ou DOWN. Já nas interfaces dos ativos de rede que estão conectados na infraestrutura, será aplicado, via protocolo de gerenciamento snmpv3 a entrada e saída dos dados, porque os dados trafegados na rede serão criptografados e o protocolo snmpv2 passa sem criptografia.

Monitoramento das Interfaces dos roteadores e Switch será usado o protocolo de gerenciamento SNMPV2, devido os equipamentos usados na implementação, não possuir suporte para SNMPV3. E as interfaces dos Servidores e computadores, serão usadas o protocolo de segurança SNMPV3, por possuir criptografia e autenticação.

Com a implantação do Sistema de monitoramento no ambiente Educacional realizado será possível ter o controle dos equipamentos para estar sempre à frente dos possíveis problemas que possam acontecer.

O Projeto proposto está organizado na seguinte forma: Capitulo 1 no texto acima mostra detalhes e planejamento da execução do projeto, onde o administrador do sistema poderá garantir o controle dos ambientes de uma forma segura.

No capítulo2, parte mais extensa, onde apresenta resumidamente os resultados de estudos e pesquisas realizadas. No capítulo3 são procedimentos, métodos e técnicas para realização do projeto. Logo a seguir nos próximos capítulos são as partes finais do projeto validando e concluindo a implantação da ferramenta de monitoramento em ambiente educacional.

1.1Definição do Tema ou Problema

Em ambientes educacionais, nas aulas ministradas em laboratórios de informática e setores que usam computadores, estão conectados diversos dispositivos de redes, como switches, roteadores, desktops, servidores, entre outros. Como esses ambientes são geralmente complexos, ou seja, quando esses dispositivos apresentarem falha ou um problema crítico e essencial que o administrador fique sabendo para que possa tomar ações o mais rápido possível, isso podem acontecer por diversos fatores como cabos de redes desconectados, mal encaixados, danificados, placas de rede com mau funcionamento, problemas de hardware (físicos), software (lógicos), entre outros. (WojciechKocjan,2008)

Conforme (TURNBULL, 2006), os profissionais de TI não têm mais tempo de individualmente analisar cada log., cada configuração, cada variável dos sistemas e aplicações aos quais eles são responsáveis. Eles precisam de ferramentas que automaticamente monitorem as características dos ativos os quais eles são responsáveis e que detectem anomalias, avisando-os proativamente quando essas falhas acontecem. Logo, essas redes precisam de ferramentas que permitam verificar se equipamentos, serviços e aplicações estão funcionando corretamente, permitindo uma ação rápida por parte dos administradores quando situações anômalas forem detectadas.

Desta forma será apresentado o Nagios Core, versão 4.4.1 como uma ferramenta de monitoramento que irá verificar constantemente o status dos computadores detectando e relatando qualquer sistema e serviços que não esteja

funcionando corretamente, para que atue de forma proativa resolvendo os possíveis problemas, sem que o usuário perceba.

1.2 Delimitações do Trabalho

Esse projeto tratará do uso do sistema de monitoramento Nagios, nos Servidores, roteadores, switch, computadores dos laboratórios e salas de informática, que existem no ambiente educacional, utilizados pelos alunos durante os horários ministrados pelos professores possibilitando a coleta de informações. Apesar de a ferramenta possuir centenas de componentes para fornecer o monitoramento de praticamente todas as aplicações. Este projeto está delimitado claramente em coletar informações dos componentes dos computadores que estão nos laboratórios e salas de informática e servidores como: HD, Memória, Processador com os sistemas operacionais windowsserver2012R2, Windows 10 e Linux, coletar informações dos componentes de interconexão e conectividade como: Switches e roteadores que estarão sendo monitorados pelo sistema de monitoramento Nagios.

1.3 Objetivos

Os objetivos dividem-se em: geral e específicos.

1.3.1 Objetivo Geral

O objetivo é implantar a ferramenta Nagios para monitorar ativos de rede em ambiente educacional.

1.3.2 Objetivos Específicos

a) Implementar o gerenciamento dos elementos lógicos e físicos da rede;
b) Fornecer subsídios para que o responsável pelo monitoramento da rede educacional que atue pro ativamente sobre as falhas que podem ocorrer no ambiente;
c) Aumentar a satisfação dos usuários em relação aos serviços prestados.

1.4 justificativa

A motivação desse projeto é a necessidade de ter um sistema de monitoramento para coletar informações dos serviços de rede,SMTP, HTTP, DNS, DHCP E ICMP, recursos da máquina, exemplo: uso do disco, carga de processamento e memória,equipamentos conectados na rede como: roteadores, switches, servidores e estações no ambiente educacional, para fornecerem alertas dos eventos gerados pela indisponibilidade dos itens monitorados,pois as instituições possuem laboratórios e salas com computadores e switches conectados na rede, onde são imprescindíveis para manter a disponibilidade desses serviços.

Sendo assim, o sistema de monitoramento, facilitará a verificação e a identificação dos problemas possibilitando não apenas o reparo como também a prevenção dos mesmos com ações de forma proativa, dando condições necessárias para que o professor tenha um bom desempenho em ministrar a aula e o aluno tenha um equipamento em boas condições para que não seja prejudicado.

A contribuição desse projeto é disponibilizar para pesquisa e de forma simples o passo a passo da implementação do sistema de monitoramento no ambiente educacional, para que futuramente auxiliam em novas implementações e instalações não só para ambientes educacionais, mas sim em ambiente coorporativo.

2 REVISÃO BIBLIOGRÁFICA

O presente projeto irá discorrer sobre a utilização do Software Nagios Core lançado em 1999 por Ethan Galstad. A ferramenta é capaz de monitorar de forma preventiva ativos de redes como servidores, estações, banda da rede/Internet, espaço em disco dos PCs, servidores, temperatura de ambientes, dispositivos UPS, entre outros, desde que sejam “inteligentes”. (OLIVEIRA, 2014). Detectam de uma forma geral problemas que ocorrem na infraestrutura em empresas de pequeno médio e grande porte. No presente projeto, será utilizada para monitoramento de ambiente educacional a qual possui computadores interligados em uma rede sendo utilizado nos laboratórios de informática ou setores que usam computadores. Pode

diagnosticar falhas antes que ocorram problemas nas redes ou nos serviços os quais se está monitorando.

2.1 Gerência de rede

A Gerência de redes pode ser definida pelas tarefas de “Monitoramento” e “Controle”, consistindo na troca de dados entre os processos gerente e agente. (TEIXEIRA, 1999). O administrador ou responsável pela rede precisa de ummétodo de controle a fim de monitorar, testar, consultar e analisar os componentes de hardware e software das maquinas conectadas. A idéia é garantir aos usuários a qualidade e disponibilidade dos serviços tanto físicos como lógicos. (STALLINGS, 1998).

Nos primórdios das redes de computadores, o ‘gerenciamento de rede’ era algo de que nunca se tinha ouvido falar. (Kurose Ano 2010). Se alguém descobrisse um problema na rede, poderia realizar alguns testes, como ping para localizar a fonte do problema e, em seguida, modificar os ajustes do sistema, reiniciar o software ou o hardware. (James Kurose e Keith Ross Ano 2009).

A arquitetura de um sistema de gerenciamento de rede permite ao administrador verificar os dispositivos interligados à rede em um ambiente computacional, a qual os ativos de rede e serviços dos computadores devem ser controlados e monitorados para garantir aos usuários a qualidade e disponibilidade do serviço. Essas ações podem ser definidas como um conjunto de ferramentas integradas para o monitoramento e controle, oferecendo uma interface única para coletar e visualizar o status da rede.

Segundo Kurose e Ross 2014 o gerenciamento de rede possui3 componentes básicos, que são principais para o monitoramento e controle: entidade gerenciadora (Gerente), dispositivo gerenciado (Agente), protocolo de gerenciamento de rede e Base de Informações Gerenciais (MIB).

2.1.1 Modelo OSI/TCP/IP

Semelhante ao modelo OSI, o modelo TCP/IP é organizado camadas. Cada camada utiliza os serviços fornecidos pela camada, com a intenção de oferecer um

serviço de melhor qualidade, modelo TCP/IP foi definido com quatro camadas ao invés de sete camadas como no modelo OSI.

Tabela 1: Modelo OSI X Modelo TCP IP

Modelo OSI	Modelo TCP IP
Aplicação	Aplicação
Apresentação	
Sessão	
Transporte	Transporte
Rede	Internet
Enlace	Acesso a Rede
Física	

Fonte: Produzida pelo autor

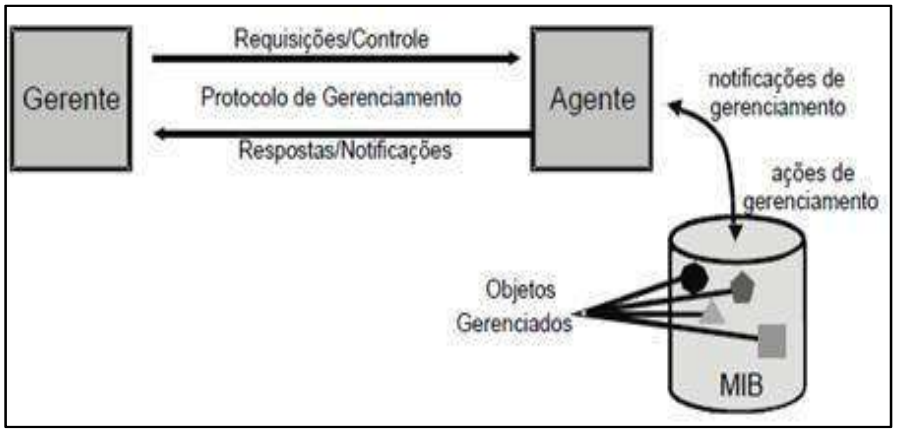
Tabela 1 acima demonstra o comparativo do Modelo OSI x Modelo TCP IP, aonde a camada OSI possuem 7 camadas e o modelo TCP IP possuem 4 camadas.

2.2 Entidade gerenciadora

Software Manager (Gerente) é um software instalado no servidor, para que seja executado pelo administrador da rede ou responsável, aonde irá monitorar e controlar a coleta de informações geradas por esses dispositivos que estão configurados no sistema. Os gerentes ou administradores de redes são as pessoas responsáveis pelo monitoramento e controle dos sistemas de hardware e software (STALLINGS, 1999).

Estações de gerência são as que conversam diretamente com os agentes nos elementos gerenciados, podendo monitorá-los ou controlá-los. Além disso, a estação de gerencia oferece uma interface em que usuários autorizados podem gerenciar a rede.

Figura 1: Troca de Informações entre Gerente e Agente



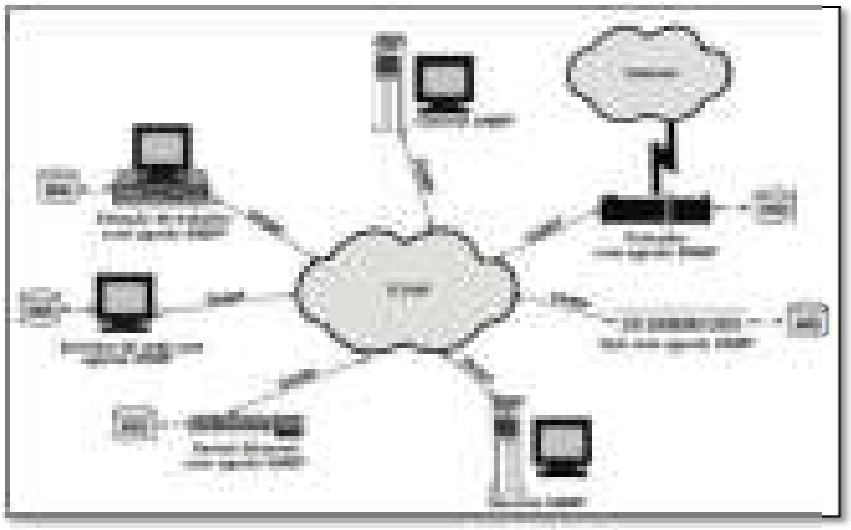
Fonte: (Oliveira Esdras,2015).

Conforme a Figura 1, podemos ver que a entidade gerente faz requisições à entidade agente, através de um protocolo de gerenciamento. O agente por sua vez, consultará uma base de objetos gerenciados chamada MIB (Master Information Base).

2.3 Entidade gerenciada

Software Agent (Agente) é instalado em ativos de rede para obter informações dos dispositivos e diagnosticar possíveis problemas para o encaminhando de relatórios. (STALLINGS, 2009). Esse gerenciamento de informações tem a finalidade de interagir com o sistema de gerência para responder as requisições de informações recebidas. A realização do gerenciamento pode ser nos computadores (estações de trabalho), e nos processadores de comunicação (Switches, roteadores, no-breaks e Ar condicionado entre outros, (Cisco 2016).

Figura 2 : Redes de Informações entre Gerente e Agente



Fonte: (Oliveira Esdras,2015).

Conforme a Figura 2, podemos ver as entidades gerenciadas (ativos de rede), transportando informações para atenderas solicitações enviadas pelo gerente através do protocolo SNMP, para que a entidade gerenciadora (gerente) colete as requisições da entidade gerenciada.

2.4 Protocolos de gerenciamento de redes

Os protocolos de gerenciamento de rede que está localizada na camada de aplicação, são arquiteturas para monitorar e controlar as atividades e os recursos, tanto de hardware quanto de software,como por exemplo, o CMIP (Common Management Information Protocol), o SNMP(Simple Network Management Protocol – Protocolo Simples de Gerência de Rede) e diversos protocolos proprietários.(KUROSE e ROSS, 2005). Todos realizam as trocas de informações através de agentes e gerentes. Porém o protocolo CMIP (Common Management Information Protocol)é definido pelo padrão OSI, que especifica de forma completa e mais segura exigindo mais recursos em uma infraestrutura, e o protocolo SNMP (Simple Network Management Protocol – Protocolo Simples de Gerência de Rede)padrão TCP/IP e o mais utilizado em gerenciamento de redes, por ser compatível pela maioria dos equipamentos e mais conhecido pela forma simples de implantar na infraestrutura, sem exigir recursos, mas suficientes para resolver os difíceis problemas (KUROSE e ROSS,2005).

Tabela 2: Modelo SNMP X Modelo OSI

Quesito	Modelo SNMP	Modelo OSI
Complexidade	Simples	Complexa
Tipos de Redes em que é implantado	Redes mais simples	Redes mais complexas
Padrão de Gerenciamento de Redes	Internet	Base do Modelo TMN
Utilização	Amplamente utilizado	Pouca utilização
Transporte	Não orientado a conexão (utiliza o UDP)	Orientado a conexão
Arquitetura	Modelo Agente – Gerente	Modelo Agente – Gerente
Operação	Comando/Resposta e Trap	Comando/Resposta e Trap

Fonte: (Oliveira Esdras,2015).

Tabela 2 acima demonstra o comparativo do Modelo SNMP x Modelo OSI, levantando as características principais de cada um deles.

2.4.1 Protocolo de gerenciamento SNMP

Simple Network Management Protocol (SNMP),protocolo simples de gerenciamento foi desenvolvido em 1988, para permitir o gerenciamento de dispositivos de IP(Internet Protocol), para que possam ser gerenciados remotamente ,fornecendo aos responsáveis pelo seu monitoramento um conjunto “simples “de operações. (DOUGLAS R. MAURO E KEVIN J. SCHMIDT, ANO 2001).

O conjunto simples de operações são informações coletados dos dispositivos que estão sendo monitorados(agentes). Essas operações obtidas pelo protocolo SNMP, Simple Network Management, permitem ao administrador alterar o estado de alguns dispositivos ou enviar informações quando ocorrer umevento, por exemplo: encerrar uma interface em um roteador ou verificar a velocidade de uma interface Ethernet e quantidade de trafego que entra e sai de uma interface. (DOUGLAS R. MAURO E KEVIN J. SCHMIDT, ANO 2001).

E possível utilizar o SNMP, para gerenciar e monitorarhospedeiros, servidores de terminais, sistemas Linux, Windows,impressoras,no-breaks(UPS), temperatura e sobrecarga da CPU, roteadores, switches e interface que permite o acionamento dos dispositivos. (Douglas & Kevin 2005).

Segundo David Josephsen 2007, o SNMP (Simple Network Management Protocol, é um dos pilares da monitoração e compatível em quase todos os dispositivos de computação.

Protocolo SNMP utiliza UDP (User Data Protocol), não orientado a conexão, como protocolo de transporte na comunicação entre NMS e Agente, para passar as informações. (Douglas R. Mauro and Kevin J. Schmidt,2005).

Segundo Douglas R. Mauro and Kevin J. Schmidt, 2005, as portas usadas por padrões são:

- UDP porta 161 – para se comunicar com o agente.
- UDP porta 162 – para enviar informações do agente para o gerente.

Figura 3 : Relacionamento NMX X Agent

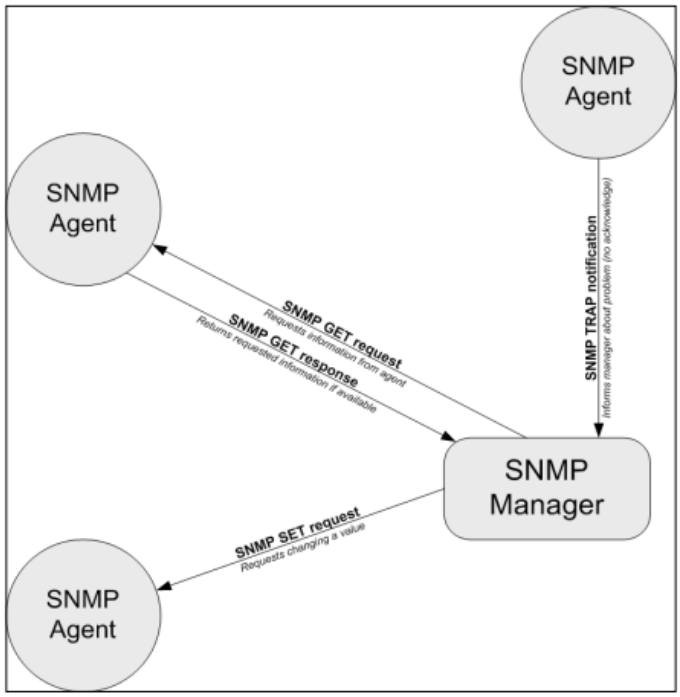
Fonte :(Douglas R. Mauro and Kevin J. Schmidt, 2005).

A Figura 3acima demonstra a base para toda comunicação do TCP/IPondeo NMS (Network Management System) busca informações no agente ou por recebimento de Trap enviada pelo agente.SegundoDouglas R. Mauro and Kevin J. Schmidt, 2005 trap e a resposta vinculada a ocorrência de um evento como: queda e recuperação de enlace e falha de autenticação e perda de dados.

De acordo com Wojciech Kocjan2014, as comunicações usadas pelo SNMP ocorrem quando um gerente envia solicitações para um agente (GET), nas quais o gerente deseja recuperar informações de um agente. Se a informação precisar ser modificada um SET pedido é enviado.

Segundo WojciechKocjan2014, outro tipo de comunicação é quando um TRAP SNMP é enviado, isso acontece no momento que um agente deseja notificar um gerente de um problema. Um agente precisa saber o IP endereço do gerente para enviar as informações.

Figura 4: Ilustração dos possíveis tipos de comunicação SNMP



Fonte: (WojciechKocjan 2014).

A Figura 4 demonstra conjunto de possíveis operações do SNMP, no qual o comando get request busca os valores de uma variável especifica, armazena operações; o comando get response responde a uma operação de busca e armazena operações; o comando set request armazena um valor em variável especifica é o comando Trap notification envia resposta acionada por um evento.

2.4.2Versões SNMP

O IETF- Internet Engineering Task Force é o órgão responsável por publicar solicitações para comentários (RFCs-Request for Comments) que são especificações aprovadas para uma IP reino IP possuem três versões SMP,(Douglas R. Mauro and Kevin J. Schmidt,2005).

- SNMP v1

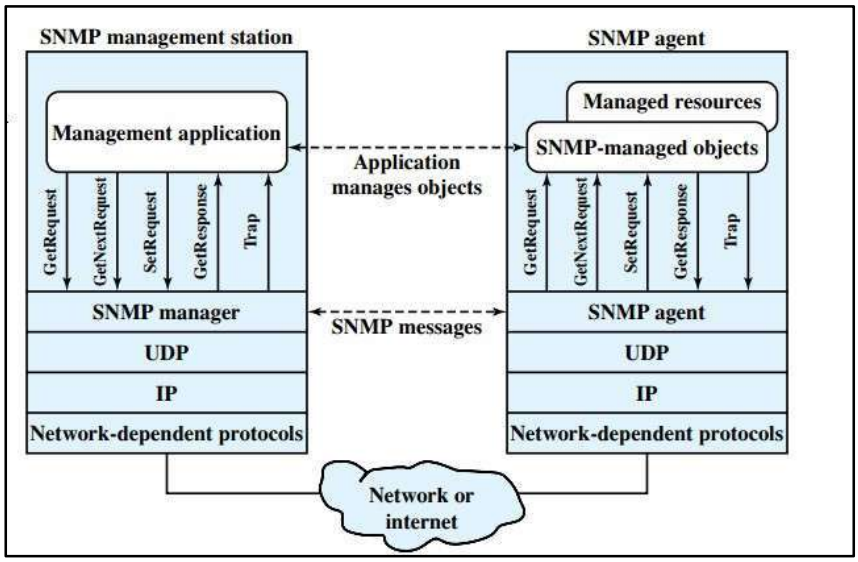
- SNMP v2
- SNMP v3

2.4.2.1SNMP v1

O SNMPv1 é definido na RFC 1157.A segurança do SNMPv1 é baseada em comunidades, strings de texto simples que permitem qualquer aplicativo baseado em SNMP ganhar acesso as informações de gerenciamento de um dispositivo. (Douglas R. Mauro and Kevin J. Schmidt,2005).

Padronizada em 1990 suportou quatro operações básicas: Get, GetNext,Set e Trap. A operação Get é usada para ler o valor da entrada MIB; o comando Get Next é usado para obter a próxima entrada de uma tabela de entradas e o comando Trap é usado para enviar uma notificação a um agente. (Dinesh Chandra Verma,2009).

Figura 5: Papel do SNMPv1



Fonte: .(William Stallings,2007).

A Figura 5 acima demonstra uma analise detalhada do protocolo SNMPv1, de uma estação de gerenciamento com 3 tipos de mensagens SNMP que são emitidas em nome de aplicativos de gerenciamento Get Request, Get Next Request e Set Request.Todas as três mensagens são reconhecidas pelo agente na forma de uma mensagem da Get Reponse, onde é passada para aplicação de gerenciamento.

As solicitações são enviadas para porta UDP161,enquanto o agente envia traps para a porta UDP 162.

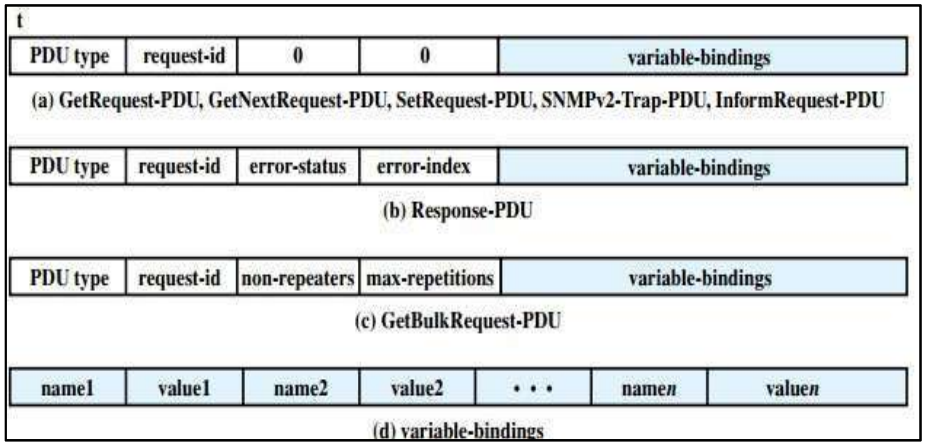
2.4.2.2 SNMP v2

O SNMPv2é definido nasRFC3416,RFC- 3416.RFC- 3417 e RFC- 3418, baseada em string de comunidade.(Douglas R. Mauro and Kevin J. Schmidt,2005).

As operações Get, GetNext e Set usadas no SNMPv1 são as mesmas usadas no SNMPv2, porem o SNMPv2 vem com duas novas operações de protocolo são eles: GetBulk e Inform. (Cisco Systems,2005).Operação Getbulk , permite a recuperação de todas as entradas na tabela em uma única operação melhorando em termos de desempenho e segurança,a operação Informe a confirmação do recebimento da camada de trap (WojciechKocjan 2008).

O SNMPv2 fornece uma estrutura onde aplicativos de gerenciamento de rede podem ser construídos. SNMPv2, possui no sistema de gerenciamento de rede um banco de dados de informações, conhecido como MIB.(WojciechKocjan 2008).

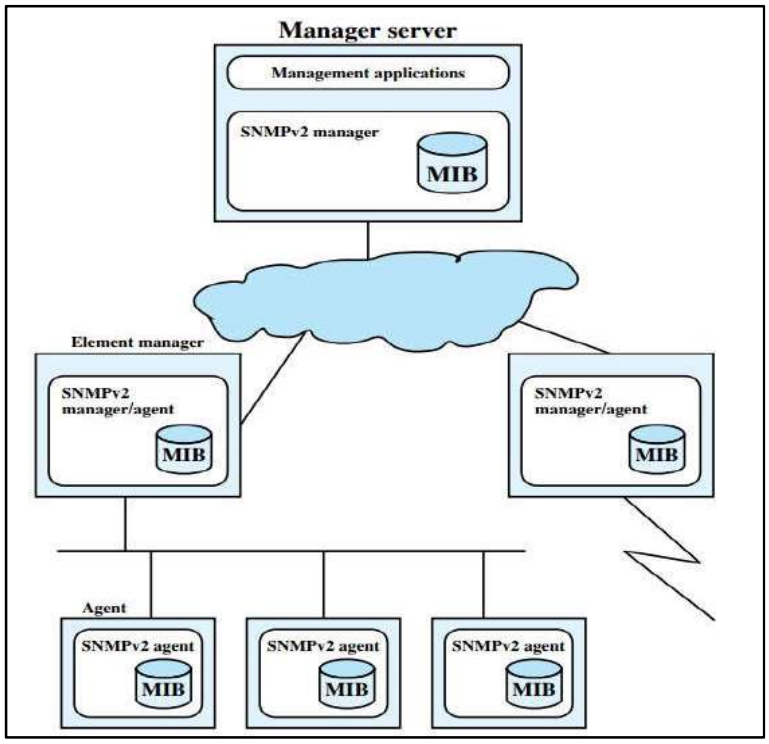
Figura 6: Configuração Gerenciada SNMPV2



Fonte:.(William Stallings,2007).

A Figura 6 acima ilustra um sistema de gerenciamento usado para trocar as informações, onde cada agente possuem um banco de dados de informações MIB, que geralmente são úteis para o gerenciamento de rede.

Figura 7: Configuração Gerenciada SNMPv2



Fonte: .(William Stallings,2007).

A Figura 7 acima ilustra sete tipos de PDUs que podem ser transportadas em uma mensagem SNMP, as PDUsGetRequest , GetNextquest e GetBulkRequest são todos enviados de um gerente para um agente para buscar informações de um ou mais Objetos MIB no dispositivo gerenciado do agente.

2.4.2.3 SNMP v3

Segundo David Josephsen 2007, o IETF-Internet EngineertingTask Force, terminou o trabalho no SNMPv3 em março de 2002, descrito no RFC- (Request for Commets) 3410 e RFC- (Request for Commets) 3418.

SNMPv3 envia pacotes texto puro e tem autenticação forte via MD5 ou SHA, que possuem sessões criptografadas e autenticação forte onde somente os receptores autenticados podem dês criptografar a mensagem (David Josephsen 2007).

A versão SNMPv3, abandona a noção de gerentes e agentes, nessa versão são chamados de entidades, esses novos conceitos definem arquitetura em vez de um conjunto de mensagens (Douglas R. Mauro and Kevin J. Schmidt).

Complementando SNMPv3 versão mais aprimorado que o SNMPv2, inclui autenticação, privacidade e controle de acesso, um dos quadros de segurança do SNMPV2.(WojciechKocjan 2008).

Mecanismos utilizados no SNMPv3

- Criptografia: Mecanismo DES (Criptografia de dados de padrão) um sistema onde usuário deve ser conhecido pela chave secreta pela entidade receptora, onde podem ser tanto MD5 quanto SHA, (KUROSE e ROSS,2005).
- Segundo Behrouz A. Forouzan, criptografia pode ser usada para autenticação do emissor e receptor da mensagem entre si, isso quer dizer que,para ter acesso aos recursos de um sistema primeiro deve receber uma autorização.
- Autenticação: Mecanismo Mensagem Authentication Code (MAC), fornece autenticação e proteção contra adulteração onde o MAC requer o remetente e receptor (KUROSE e ROSS,2005).
- Segundo Behrouz A. Forouzan, autenticação e o processo realizado antes ganhar acesso aos recursos do sistema.
- Controle de Acesso: Mecanismo baseado em visão (VACM-View-based Access Control Model), que controla quais informações de gerenciamento de rede podem ser consultadas (KUROSE e ROSS,2005).

2.5 MIB - Management Information Base

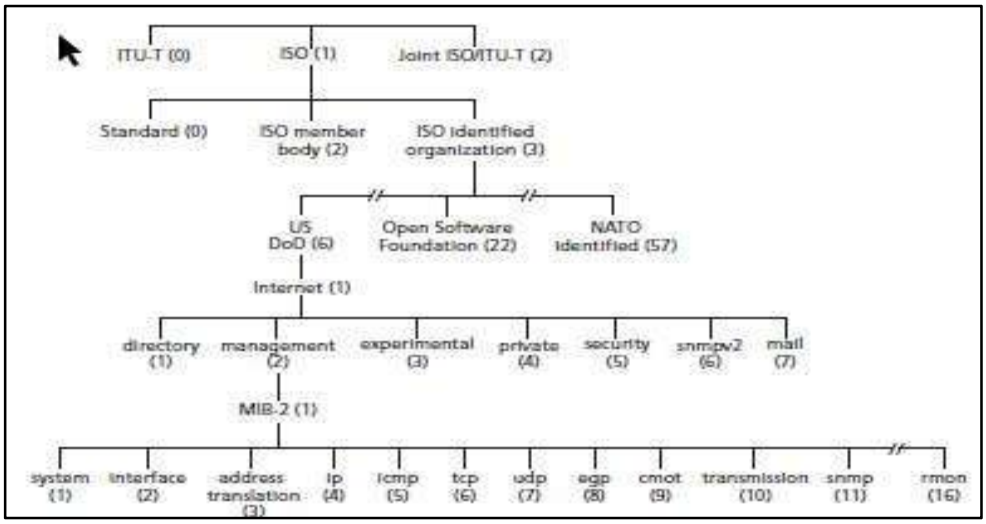
Segundo Thomas A. Limoncelli 2004 existem variáveis para quase tudo e todo tipo de tecnologia, há MIB - Management Information Base padrão para dispositivos Ethernet, dispositivos DSL, dispositivos ATM,dispositivos SONET e mesmo tecnologias sem rede: discos, impressoras, CPUS, processos e assim por diante.

Cada objeto de gerenciamento possui um identificador de objeto ou definições que definem estrutura dos dados de gerenciamento disponíveis nas entidades gerenciadas, esse identificador e o nome exclusivo hierarquicamente estruturado aonde a estrutura e representada por números inteiros separados por períodos. (DineshChandraVerma 2009).

A MIB para estação de gerenciamento funciona uma coleção de ponto de acesso no agente, aonde esses valores podem ser consultados pela entidade gerenciadora enviando mensagens SNMP (William Stallings,2007).

Os objetos são nomeados na estrutura de nomenclatura ISO, na forma hierárquica. No topo estão ISO e a Padronização de Telecomunicações Setor da União Internacional de Telecomunicações UIT-T. (KUROSE e ROSS,2005).

Figura 8: Arvore de Identificador de Objeto



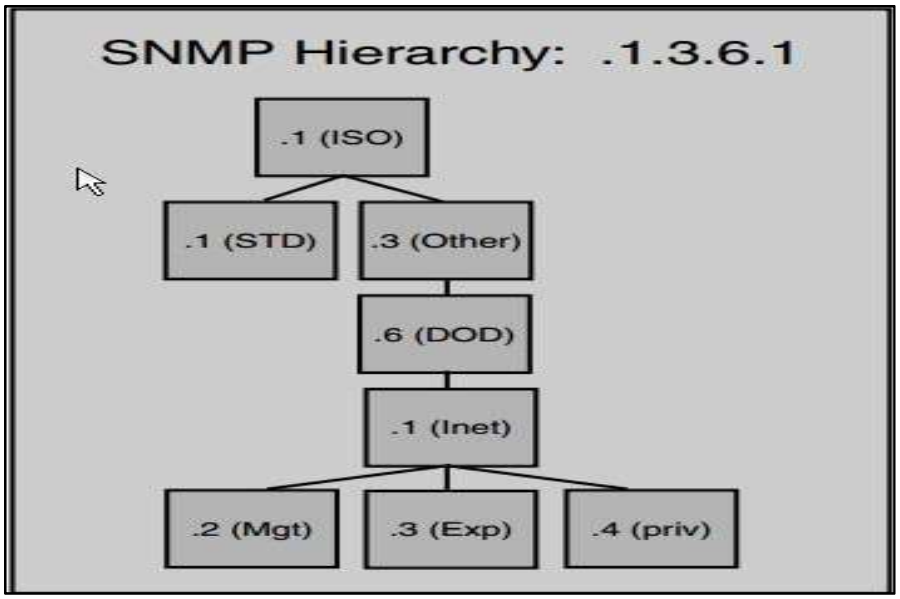
Fonte: (KUROSE e ROSS,2005).

A Figura 8 acima mostra objetos nomeados na estrutura de nomenclatura ISO, e se faz uma observação que cada ponto de ramificação na árvore tem um nome e um número que especificam o caminho até aquele ponto da arvore identificadora.

De acordo com DineshChandra Verma2009, o mapeamento realizado na estrutura de gerenciamento pelo agente SNMP e uma das principais funções de maneira em que os dados são armazenados localmente.

Normalmente todos OIDs MIB começam 1.3.6.1, a partir do quinto numero inteiro, a hierarquia continua se tornar mais especifica, é 1 se o grupo for para diretório OSI, 2 se o grupo relaciona-se ao gerenciamento de rede, 3 se for identificador experimental e 4 para privado (DineshChandra Verma2009).

Figura 9: Hierarquia SNMP



Fonte: (David Josephsen 2007).

A Figura 9 acima demonstra uma estrutura hierárquica, a qual 1 (ISO) é a arvore padrão ,3 (Other) ou (org) organizations um nó marcador para todos as organizações internacionais ,6 (DOD) Department of defense nó do departamento de defesa dos EUA ,1 identifica a Internet Força Tarefa de Engenharia e abaixo 3 categorias mais utilizadas.

2.5.1 MIB –Experimental

Subgrupo experimental 1.3.6.1.3, usado para nós que possivelmente se tornarão IETF. Ramo experimental habilita administradores usar OIDs experimentais sem causar conflitos com OIDs existentes. (David Josephsen 2007).

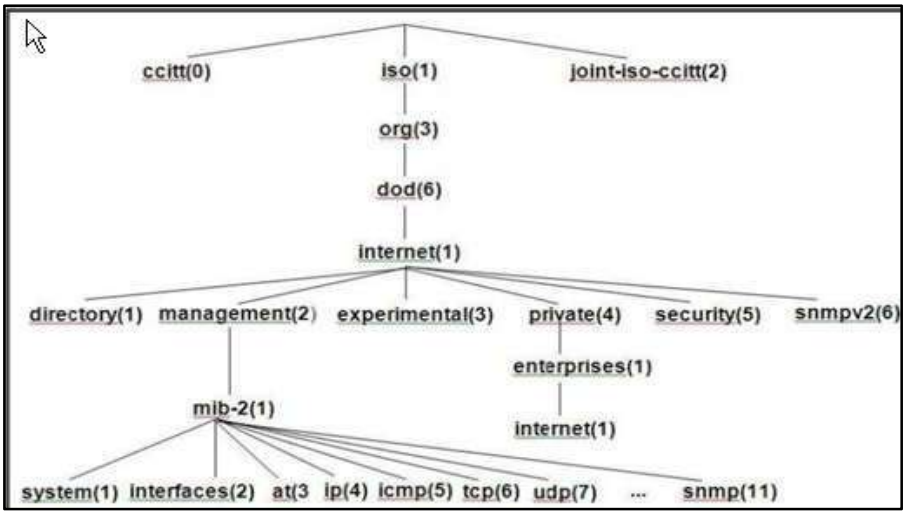
2.5.2 MIB – Privada

Subgrupo privado 1.3.6.1.4, usado para empresas, podendo definir seus próprios MIBs proprietários. (David Josephsen 2007). Segundo (KUROSE e ROSS,2010), sob a ramificação privada foi encontrada uma lista [IANA 2009 b] dos nomes e códigos corporativos privados de empresas privadas.

2.5.3 MIB – MIB II

Subgrupo do gerenciamento 1.3.6.1.2 e mib-2 1.3.6.1.2.1 da estrutura hierárquica encontramos as definições dos módulos MIB padronizados.
(KUROSE e ROSS,2010).

Figura 10: Arvore de identificador de Objeto MIB 2



Fonte: Pinheiro Ricardo, 2015.

A Figura 10 acima demonstra uma estrutura iso. org. dod.internet.mgmt.mib-2→ 1.3.6.1.2.1 com base de informações de gerenciamento , versão 2 , o qual cada agente tem sua própria MIB2.

- **MIB-II os seguintes grupos:**

Grupos	**Informações**
• **system(1)**	Sistema de operação dos dispositivos da rede
• **interfaces(2)**	Interface da rede com o meio físico
• **addresstranslation(3)**	Mapeamento de endereços IP em endereços físicos
• **ip(4)**	Protocolo IP

- **icmp(5)** Protocolo ICMP
- **tcp(6)** Protocolo TCP
- **udp(7)** Protocolo UDP
- **egp(8)** Protocolo EGP
- **cmot(9)** Protocolo CMOT
- **transmission(10)** Meios de transmissão
- **snmp (11)** Protocolo SNMP

2.6Monitoramento

O monitoramento de um sistema informático é definido como o processo para obter informações de status e configuração dos vários elementos conectados na rede. (Verma,2009).

Segundo Verma, 2009, para um gerenciamento requer uma variedade de dados, para que os tipos de informações sejam monitorados.

Para fins de monitoramento o gerenciamento de rede exige a capacidade monitor, testar, pesquisar e configurar os componentes de hardware e software para que o administrador consiga coletar dados (KUROSE e ROSS, 2010).

A informação coletada pode ser enumerada em grupos lógicos típicos de informações monitoradas para cada elemento de um sistema gerenciado: como por exemplo: Informações do status, informações da configuração, estatísticas de uso e desempenho, informações de erro e informações de topologia. (Verma, 2009).

A estrutura do monitoramento utilizados na gestão e descrita em 5 camadas de monitoramento: Relatório, processamento de dados, banco de dados, Processamento de dados e coleção de dados. (Verma, 2009).

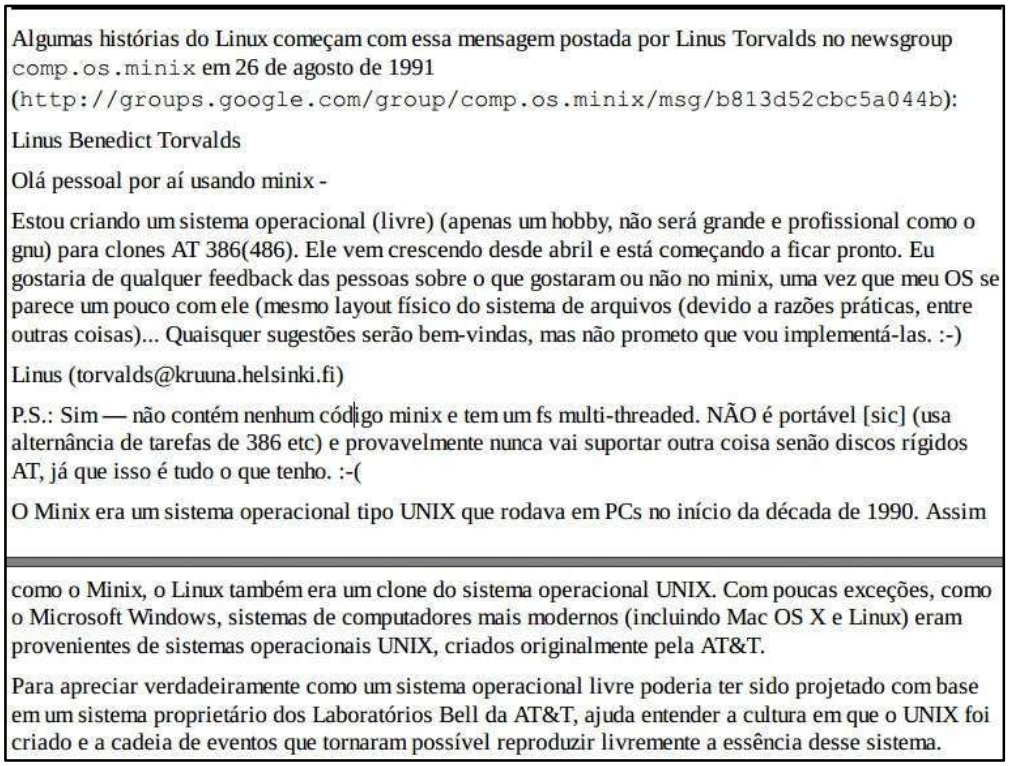
2.7 S.O. Linux

Segundo CHRISTOPHER2014, Linux e um sistema operacional o qual podemos executar aplicativos nele, podendo gerenciar seu computador através de um software.

O que caracteriza os sistemas operacionais Linux são: Detectar e preparar hardware, Gerenciar processos, Gerenciar memória, Fornecer interfaces de usuário, controlar sistemas de arquivos, proporcionarem o acesso e autenticação de usuário, oferecer utilitários administrativos, iniciar serviços e Ferramentas de programação (CHRISTOPHER NEGUS, 2014).

O Sistema GNU/LINUX, originou-se em 1991, projeto pessoal de Linus Torvalds, onde o sistema ficou chamado pelo segundo nome Linux, descrito como um sistema operacional de código-fonte aberto. (CHRISTOPHER NEGUS, 2014).

Figura 11: Mensagem por Linus Torvalds



Algumas histórias do Linux começam com essa mensagem postada por Linus Torvalds no newsgroup comp.os.minix em 26 de agosto de 1991 (http://groups.google.com/group/comp.os.minix/msg/b813d52cbc5a044b):

Linus Benedict Torvalds

Olá pessoal por aí usando minix -

Estou criando um sistema operacional (livre) (apenas um hobby, não será grande e profissional como o gnu) para clones AT 386(486). Ele vem crescendo desde abril e está começando a ficar pronto. Eu gostaria de qualquer feedback das pessoas sobre o que gostaram ou não no minix, uma vez que meu OS se parece um pouco com ele (mesmo layout físico do sistema de arquivos (devido a razões práticas, entre outras coisas)... Quaisquer sugestões serão bem-vindas, mas não prometo que vou implementá-las. :-)

Linus (torvalds@kruuna.helsinki.fi)

P.S.: Sim — não contém nenhum código minix e tem um fs multi-threaded. NÃO é portável [sic] (usa alternância de tarefas de 386 etc) e provavelmente nunca vai suportar outra coisa senão discos rígidos AT, já que isso é tudo o que tenho. :-(

O Minix era um sistema operacional tipo UNIX que rodava em PCs no início da década de 1990. Assim como o Minix, o Linux também era um clone do sistema operacional UNIX. Com poucas exceções, como o Microsoft Windows, sistemas de computadores mais modernos (incluindo Mac OS X e Linux) eram provenientes de sistemas operacionais UNIX, criados originalmente pela AT&T.

Para apreciar verdadeiramente como um sistema operacional livre poderia ter sido projetado com base em um sistema proprietário dos Laboratórios Bell da AT&T, ajuda entender a cultura em que o UNIX foi criado e a cadeia de eventos que tornaram possível reproduzir livremente a essência desse sistema.

Fonte:(CHRISTOPHER NEGUS,2014).

A Figura 11 acima mostra um mensagem enviada pelo o próprio inventor do Linux (Linus Torvalds).

Segundo Gleydson Mazioli da Silva, o suporte ao sistema Linux é um dos mais eficientes do que qualquer programa comercial disponível no mercado.

Outra opção de suporte e através da comunidade Linux; podendo se inscrever em uma lista de discussão. (Gleydson Mazioli da Silva).

De acordo com o Gleydson Mazioli da Silva sistema Linux possui algumas características:

- Sistema Linux é livre e desenvolvido voluntariamente por programadores experientes.

- Multiusuário e Multitarefa real.
- Conectividade com outros tipos de plataforma como, por exemplo: Windows, DOS e Unix.
- Executa outras plataformas como Windows, DOS e Linux através de virtualização.

Sistema operacional Debian para gerenciar todos os pacotes de software em seu sistema usa ferramenta e pacote deb, uma distribuição Linux inicial (CHRISTOPHER NEGUS, 2014). De acordo com a DistroWatch, mais de 120 distribuições Linux se originam do Debian. Mas o maior sucesso alcançado e o ubuntu(http://www.ubuntu.com).(CHRISTOPHER NEGUS,2014).

Segundo (CHRISTOPHER NEGUS, 2014).os recursos que faltavam ao Debian , foi avançado e adicionado pela distribuição Ubuntu, por exemplo : um instalador gráfico simples e ferramentas gráficas fáceis de usar.

2.8. Breve História do Nagios

- Em 1996, Ethan Galstad cria um aplicativo MSDOS simples projetado para “pingar”, Servidores Novell Netware e enviar páginas numéricas.
- Em 1998, 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. Intuito é entrar o negócio de monitoração / serviços gerenciados.
- Em 1999, Ethan lança seu trabalho, Projeto Open Source sob o nome “NetSaint”.
- Os plug-ins que foram originalmente distribuídos como parte da distribuição do NetSaint, são logo desmembrados como um projeto separado do Nagios Plug-ins.
- Em 2002, Devido a problemas de marca registrada com o nome “Net Saint”, Ethan decide renome ar o projeto para “Nagios”. Enquanto o projeto NetSaint é movido para o projeto Nagios Plug-ins.

Fonte: https://www.nagios.org/about/history/

Nagios um sistema de monitoramento poderoso que permite com que a equipe de tecnologia possa de forma proativa identificar e resolver problemas de infraestrutura (OLIVEIRA 2014).

2.8.1Nagios e suas Versões

O Nagios possui 3 versões sendo que uma gratuita:

2.8.1.1 Nagios XI

Ferramenta comercial completa desenhada de acordo com uma base de conhecimento e implantação do Nagios em todo mundo,é possível encontrar inúmeros plug-ins pré-configurados para realizar o monitoramento de diversos tipos de serviços e equipamentos (OLIVEIRA, 2014). Software de monitoramento de rede e servidor corporativo uma solução central onde requer licenciamento.

Benefícios dessa versão Nagios XI:

- Monitoramento abrangente de Infraestrutura de TI
- Visibilidade
- Customizabilidade
- Recursos de vários inquilinos
- Planejamento proativo e conscientização
- Fácil de Usar
- Arquitetura Extensível

Requisitos de Hardware:

Figura 12: Hardware mínimo requerido todas versões do Nagios

Monitored Nodes / Hosts	Monitored Services	Hard Drive Space	CPU Cores	RAM
50	250	40 GB	1 - 2	1 - 4 GB
100	500	80 GB	2 - 4	4 - 8 GB
> 500	> 2500	120 GB	> 4	> 8 GB

Fonte: OLIVEIRA 2014

A figura 12 acima fornece especificações de hardware mínimo, algumas considerações são fundamentais, mas de preferencialmente que o servidor tenha fontes redundantes (OLIVEIRA, 2014).

2.8.1.2NagiosFusion

Requer licenciamento e oferece às empresas a capacidade de identificar e resolver os problemas críticos de forma mais eficiente na infraestrutura. Administradores que utilizam o Nagios fusion trabalham com um mecanismo de "percepção" onde avalia em tempo real uma rápida indicação visual do problema em toda infraestrutura de TI, permitindo a detecção mais rápida de um possível problema. (OLIVEIRA, 2014).

Benefícios dessa versão NagiosFusion:

- Visão Centralizada
- Monitoramento Distribuído
- Gerenciamento Descentralizado
- Compatibilidade
- Serviço gerenciado
- Integração total com o Nagios Log Server
- Escalabilidade sem limites
- Suporte abrangente ao servidor
- Visibilidade de interrupção

2.8.1.3Nagios Core (Free)

Solução popularmente conhecida, não requer licenciamento para implantação, oferece recursos principais de monitoramento. Porém necessita ser customizada para que objetivo da ferramenta seja atendido de forma esperada. (OLIVEIRA,2014) Vantagem por ser uma ferramenta Free o Nagios Core oferece é acompanhamento exaustivo, visibilidade, sensibilização, corretores de problemas e relatórios e arquitetura extensível. (OLIVEIRA, 2014)

Benefícios dessa versão Nagios Core:

- Monitoramento
- Alerta
- Resposta
- Relatório
- Manutenção
- Planejamento

2.8.2 Monitorando com Nagios

Nagios uma ferramenta para monitoramento, que verifica constantemente o status de máquinas e vários serviços desses hosts, onde objetivo principal do sistema de monitoramento é detectar e relatar qualquer host e serviço que não esteja funcionando corretamente (WojciechKocjan, 2009).

Os objetos monitorados pelo sistema Nagios são divididos em duas categorias: hosts e serviços. Hosts são maquinas físicas, por exemplo: Servidores, roteadores e hosts, enquanto serviços são funcionalidades da máquina por exemplo: servidor web (WojciechKocjan, 2009).

O software Nagiospara realizar verificações em hosts gerenciados e serviços, ele emprega plug-ins podendo ser executáveis compilados ou scripts de leitura. (Max Schubert 2008).

Segundo (WojciechKocjan, 2009) os plug-ins são responsáveis por verificar e analisar os resultados, onde a verificação do status (OK WARNING, CRITICAL ou DESCONHECIDO, e texto adicional que fornece informações detalhadas sobre o serviço.

Plug-ins são extensões independentes que permitem monitorar tudo e qualquer coisa com Nagios, por exemplo: hardware, serviços, banco de dados, sistemas operacionais, aplicativos, equipamento de rede e protocolos, são argumentos de linha de comando, que realizam uma verificação especifica onde retornam os resultados ao Nagios.((WojciechKocjan, 2009).

De acordo com site oficial do Nagios (https://www.nagios.org/projects/nagios-plugins), existem aproximadamente 50 Plug-ins oficiais do Nagios, onde esses plugins são desenvolvidos e mantidos pela equipe oficial NagiosPlugins.

Figura 13: Código de retorno Plug-ins Nagios

Service	Status	Last Check	Duration	Attempt
Current Load	OK	11-03-2011 15:43:52	2d 9h 54m 54s	1/4
Current Users	OK	11-03-2011 15:44:31	2d 9h 54m 16s	1/4
HTTP	WARNING	11-03-2011 15:45:07	0d 14h 45m 18s	4/4
PING	OK	11-03-2011 15:40:45	2d 9h 47m 1s	1/4
RHQ	CRITICAL	11-03-2011 15:45:18	0d 0h 0m 7s	1/1
Root Partition	OK	11-03-2011 15:41:22	2d 9h 52m 24s	1/4
SSH	OK	11-03-2011 15:42:00	2d 9h 51m 46s	1/4
Swap Usage	OK	11-03-2011 15:42:41	2d 9h 51m 9s	1/4
Total Processes	OK	11-03-2011 15:43:55	2d 9h 50m 31s	1/4

Fonte :Chies Rafael, 2013

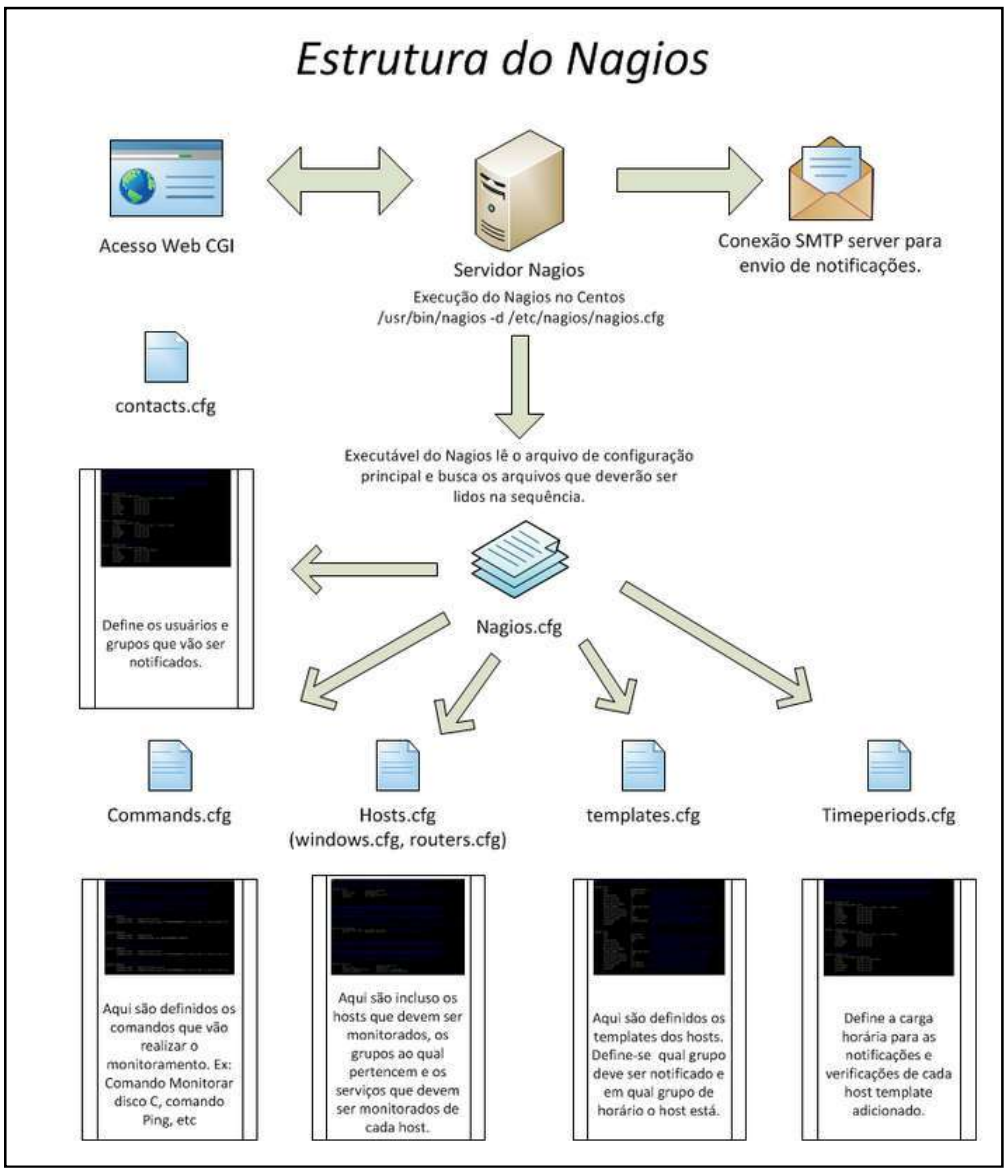
A figura 13 acima na aba do Status mostra os plug-ins elaborados com a finalidade de capturar as informações e informar ao Nagios a ocorrência de algum problema, retornando, se a situação é WARNING, CRICITAL ou OK.

2.8.3 Estrutura do Nagios

Nagios e um sistema de monitoramento de rede e de aplicação, que funciona através de arquivos de configuração, que sejam lidos e executados, ou seja, um arquivo executável responsável por fazer todas as configurações Nagios.cfg.

Conforme a figura 14 abaixo:

Figura 14: Estrutura do Nagios



Fonte: Admin, 2012

A figura 14 acima demonstra como é formada a estrutura do sistema nagios e as distribuições dos arquivos de configuração.

Os chamados de ficheiro são os principais arquivos de configuração do nagios.

- ***nagios.cfg***

  Arquivo de configuração principal do Nagios, responsável por iniciar os serviços de monitoramento.

- ***cgi.cfg***

  Arquivo de configuração dos programas CGIs localizados na pasta sbin.

- ***contacts.cfg***

  Contatos que deverão ser notificados caso alguma falha aconteça.

- ***commands.cfg***

  Contém todas as definições de comandos a serem executados pelo Nagios, desde os comandos de plug-ins até de notificação. Todos os comandos que o sistema executar, deve estar definido nesse arquivo.

- ***hosts.cfg***

  Arquivo contendo informações sobre hosts criados que serão monitorados.

- ***templates.cfg***

  Mantém modelos de configuração que podem ser utilizados como padrão.

- ***hostgroups.cfg***

  Arquivo contendo informações de hosts por grupos.

- ***timeperiods.cfg***

  Informações sobre o período de monitoramento, podem ser definidas vários períodos de monitoramento diferentes.

- ***contactsgroups.cfg***

  Contatos divididos em grupos.

- ***services.cfg***

  Serviços que deverão ser monitorados.

- ***dependencies.cfg***

  Informações de serviços que dependem de outros serviços.

- ***checkcomands.cfg***

  Definição dos comandos que podem ser executados pelo Nagios.

- ***resource.cfg***

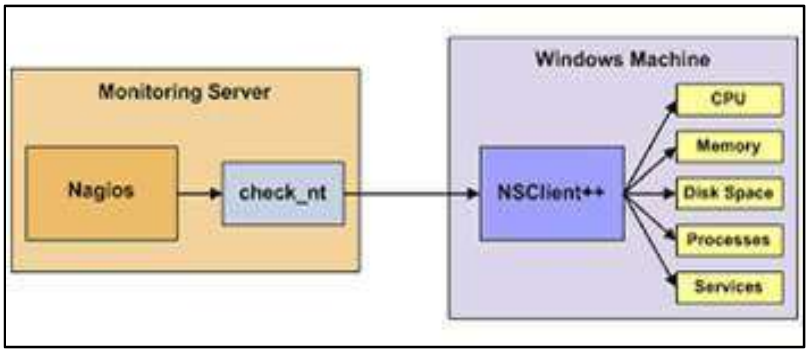
  Macros definidas pelo usuário.

2.8.4 Monitoramento Agente para Windows (pNSClient)

O pNsClient foi construído para o Nagios, mas pode ser usado em outros cenários (OLIVEIRA,2014). Um agente utilizado para realizar a coleta de dados de um host Windows depois de instalado, abre a porta 1248, permitindo que o servidor Nagios estabeleça uma conexão para coletar dados do dispositivo em tempo real. (OLIVEIRA, 2010) o Nsclient possui verificações integradas, mas o poder real vem de plug-ins e scripts externos (OLIVEIRA, 2010).

Scripts externos são os escritos para serem executados pelo Nsclient, e os resultados são enviados de volta ao servidor de monitoramento podendo assim analisar o elemento monitorado. Uma vez que o Nsclient foi projetado para trabalhar com Nagios, ele possui suporte para os vários protocolos usados por ele, e também suporte uma série de outros protocolos (OLIVEIRA, 2014) um deles é: Check_nt→Protocolo utilizado pelo sistema de monitoramento check_nt.

Figura 15: Visão Geral do Check_nt



Fonte: Ethan Galstad, 2009

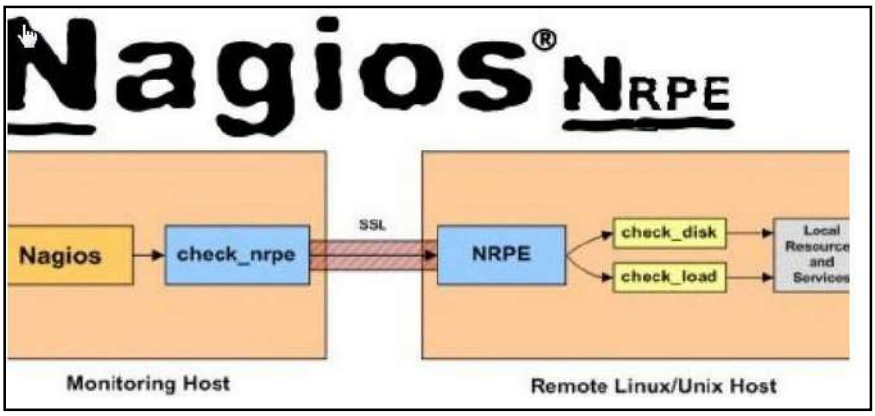
Conforme a Figura 15, podemos ver que através do plugin check_nt consulta o agente NSClient ++ em busca de informações dos serviços que estão sendo monitorados.

2.8.5 Monitoramento Agente para Linux

NRPE Nagios Remote Plugin executor, um complemento para Nagios para possibilitar o monitoramento de maquinas Linux, permite que executem plug-ins do Nagios para realizar a coleta de informações dos agentes monitorados. (OLIVEIRA, 2014).NRPE um agente que trabalha com objetivo de coletar informações e enviá-

las ao servidor Nagios irão monitorar um recurso ou serviço executando o plugincheck_nrpe, dizendo qual serviço deverá ser checado então o NRPE ira rodar o plugin para checar o serviço ou recursos requeridos.(OLIVEIRA, 2014).

Figura 16: Visão Geral do Check_NRPE



Fonte: Herrero Hector, 2017

Conforme a Figura 16, podemos ver que através do plugin check_nrpe consulta o agente NRPE em busca de informações dos serviços que estão sendo monitorados.

2.9 Wireshark

É um software para a análise de tráfego de pacotes de uma rede de computadores, aonde esta ferramenta captura informações que ocorre na rede e todos os tipos de informações de protocolo de pacotes em vários formatos. (CHRIS SANDERS, 2017).

3 DESCRIÇÃO DA SOLUÇÃO

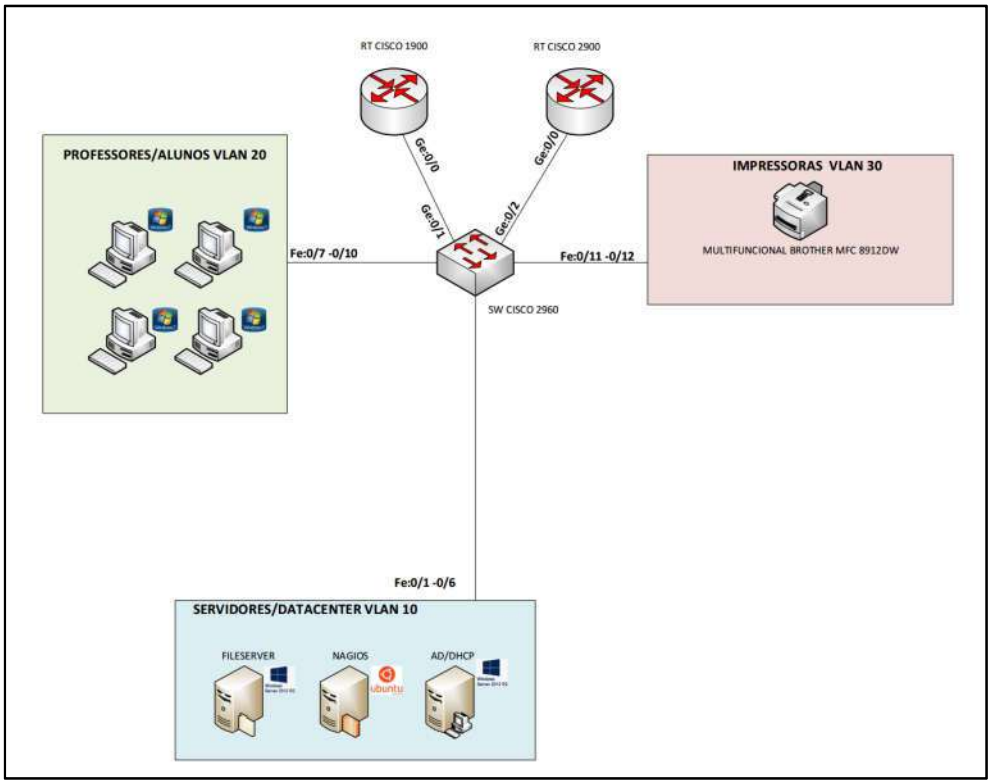
Este projeto baseia-se na busca por atender de forma proativa e preventiva, os ativos interligados no ambiente educacional e os serviços monitorados,onde o responsável pelo monitoramento da rede recebera uma notificação com a mensagem se a situação é WARNING (aviso de alerta o item monitorado),CRITICAL (quando item monitorado está em situação crítica) ou OK, no qual possibilitará que o

administrador da ferramenta haja de forma rápida na resolução de problemas, possibilitando um suporte adequado a partir do momento que o serviço ou ativo de rede apresentar falhas no monitoramento.

Foi criado um cenário utilizando método experimental simulando um ambiente educacional.

Figura 17 abaixo:

Figura 17: Cenário - Topologia



Fonte: Produzida pelo autor

A figura 17acima é uma estrutura da rede, onde todos os ativos conectados na rede serão monitorados.

A topologia esta composta por dois roteadores, Roteador Cisco 2900 e Roteador Cisco 1900 Series, que estão conectados no Switch Catalyst 2960 Series com objetivo de realizar uma redundância de links, se houver um problema no link outro assume, onde monitoramento das interfaces será realizado por via snmpv2, com objetos check_ifstatus para verificar o status da porta das interfaces de rede, ifOutOctets para monitorar taxa de bytes enviados,ifInOctetspara monitorar taxa de bytes recebido se via ping para acompanhar as variações e carga entre os links.

Protocolo SNMPV3, não foi usado devido o modelo do roteador e switch não possuir essa versão. Foram colocados Três Servidores Dell Intel Core i5 2400 3.10GHz, Memória 4,00 GB, conectados na Vlan 10 para serem monitorados e ter o controle do que está acontecendo dos mesmos.

Utilizou-se o servidor Nagios Core Versão 4.4.1, que será implementado utilizando sua instalação local na rede a partir da Vlan 10. A gerência do referido servidor será centralizada, onde funcionará como responsável pelo monitoramento de todos os ativos de rede no cenário proposto. Para realizar a coletas das informações dos ativos na rede,como por exemplo, os Servidores de rede e desktop será utilizado o agente NSClient nativo do nagios, que possibilitara obter informações de objetos como Memória, CPU, DISCO, PING,Interface das Redes,Serviço do NSClient e agente Net-SNMP Agent.

Servidor DNS (Domain Name Server), Servidor DHCP (Dynamic Host Configuration Protocol e Servidor FILE SERVER, serão monitorados os mesmos objetos via agente NSclient por ser originalmente projetado para trabalhar com Nagios, como Memória,HD, CPU, PING,já os serviços como: Net-SNMP Agent e nscp, serão monitorados nos três servidores por serem os objetos do agente instalados nos servidores para coletar informações e enviar para o Nagios.

Os Serviços DNS SERVER e NTDS, serão monitorados no Servidor DNS por serem serviços de extrema importância, ou seja, não haveria como navegar na rede acessando os sites pela URL, se os serviços estiverem parados.O serviço DHCPServer,onde distribuem automaticamente os endereços Ip, será monitorado no Servidor DHCP se o serviço parar, os computadores não vão ganhar Ip, não vão ter conectividade com a rede. O Serviço S.O.S Backup,será monitorado no Servidor FILESERVER, devido esse serviço ser o responsável pelas cópias de segurança dos arquivos. E a interface de rede dos servidores e Desktop serão monitorado a partir do agente snmpv3 em vista que o referido protocolo oferece criptografia e autenticação no tráfico de dados.

Uma impressora Multifuncional 8912dwconectada na Vlan 30 será monitorada via SNMPV2, para monitorar o consumo de tinta e o status se esta Up ou Down .

Os desktops conectados na Vlan 20,serão monitorados pelo agente NSClient como Memória, CPU, PING , HD, e as Interfaces de rede será monitorado via protocolo snmpv3 porque os dados trafegados na rede serão criptografados.

A solução proposta pela ferramenta será de realizar o monitoramento dos servidores e seus serviços, desktops, impressora e ativos de rede, possibilitando agir de forma preventiva, para eventuais problemas que possam ocorrer na infraestrutura. Sempre que houver alguma ocorrência que possa gerar um incidente, será emitido um alerta pelo Nagios em sua tela de monitoramento. Onde nestes alertas são definidas as mensagens, WARNING (AVISO), CRITICAL (INCIDENTE) ou OK, para o responsável pelo monitoramento da ferramenta. Desta forma haverá uma resposta mais rápida no tratamento das causas identificadas, solucionando os problemas em tempo hábil.

Foram escolhidos serviços como, Memória, Espaço em Disco, Ping, Status e Carga CPU, por serem os serviços fundamentais no uso do ativo de rede.

- Carga CPU →Consiste em determinar processamento à utilização da CPU, chamado processador.
- Monitorar Memória →Consiste em saber a utilização da memória.
- Monitorar Armazenamento → Consiste em saber o espaço livre em disco e espaço ocupado.
- Monitorar Ping → Saber a disponibilidade do ativo de rede.
- Monitorar Uptime → Saber quanto tempo está ligada.
- Monitorar Serviço Net-Snmp→ Se está ativo Up ou Down, serviço snmpv3.
- Monitorar processos →Monitora total de processos que esta sendo executada no computador.

4 METODOLOGIA

Foi utilizado o método de pesquisa bibliográfica, a fim de coletar informações de livros, sites e trabalhos acadêmicos, para adquirir conhecimento e embasamento teórico.

Reunindo todas essas informações, foi atingido o objetivo do projeto, que foi a implementação da ferramenta de monitoramento Nagios Core versão 4.4.1e demonstrar as suas respectivas funcionalidades do sistema, mostrando também benefícios de segurança e trafego.

4.1 Cenário

Com base nas informações coletadas nos documentos estudados sobre a ferramenta Nagios foi criado um cenário simulando um ambiente educacional, onde será realizado o monitoramento dos ativos presentes no cenário.

Nesse cenário foi implementado e configurado o sistema de monitoramento nagios versão 4.4.1, onde o servidor ficara centralizado e realizando o monitoramento de todos ativos mencionado no cenário e serviços.

Com intuito de demonstrar que sem um sistema de monitoramento adequado, não é possível diagnosticar se ativo de rede ou serviço está ou não funcionando.

4.2 Documentação - Instalação e Configuração do Nagios

Download ,

Através do link http://www.nagios.org/download, pode ser realizado o download do Nagios Core, conforme demonstra APÊNDICE A - Download do Nagios.

Instalação Nagios Core,

Realizar o download da versão do Nagios Core, conforme demonstra APÊNDICE B - Download do Nagios Core..

wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.1.tar.gz.

Realizar o download dos Plug-ins, conforme demonstra APÊNDICE C - Download Plug-ins.

wget https://nagios-plugins.org/download/nagios-plugins-2.2.1.tar.gz,

Descompactar o arquivo, conforme demonstra APÊNDICE D – Descompactar arquivos.

tar xzf nagios-4.4.1.tar.gz

tar xzf nagios-plugins-2.2.1.tar.gz

Instalar dependências, conforme demonstra APÊNDICE E – Instalação dependências.

apt-get install apache2 build-essential php libgd-dev unzip postfix s-nail unzip libapache2-mod-php7.0 traceroute,(essas bibliotecas fazem com que o nagios

funcione, pacote apache2 responsável por disponibilizar as páginas, pacote build-essential conjunto de pacotes e bibliotecas de compilação, pacote php linguagem de programação utilizada pelo nagios demais pacotes são pacotes como unzip e postfix são extras,

Criar do usuário e grupo para Nagios, conforme demonstra APÊNDICE F – Criar Usuario.

```
# useradd  nagios
# groupadd nagcmd
# passwd nagios
# usermod -a -G nagcmd nagios
# usermod -a -G nagios, nagcmd www-data
```

Compilar arquivo dentro da pasta nagios-4.4.1, conforme demonstra APÊNDICE G – Compilar Arquivo

```
# cd nagios-4.4.1/
#./configure  --prefix=/usr/local/nagios  --with-httpd-conf=/etc/apache2/sites-enabled/
--with-command-group=nagcmd --with-mail=/usr/bin/mail,
# make all
# make install
# make install-init
# make install-config
# make install-commandmode
# make install-webconf
# cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/
# chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers
```

Comando de teste, para verificar se estão ok as configurações, conforme demonstra APÊNDICE H– Comando de Teste

```
#  /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

Em ambos os casos o resultado esperado é o seguinte:

```
Total Warnings: 0
Total Errors:   0
```

Instalação Plugins , conforme demonstra APÊNDICE I– Instalação Plugins

```
# cd nagios-plugins-2.1.4/
#. /configure --with-nagios-user=nagios --with-nagios-group=nagios
```

#make && make install

Criar usuário para acessar a Interface do Nagios pela Web, conforme demonstra APÊNDICE J– Acessar Interface do Nagios pela Web

htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

Habilitar2 módulos - CGI e rewritee reinicie o Apache para funcionar , conforme demonstra APÊNDICE L– Módulos CGI - REWRITEE

a2enmod rewrite cgi

/etc/init.d/apache2 restart

cd /etc/init.d/

rm -rf nagios

cp -p skeleton nagios

#nano nagios

DESC="Nagios"

NAME=nagios

DAEMON=/usr/local/nagios/bin/$NAME

DAEMON_ARGS="-d /usr/local/nagios/etc/nagios.cfg"

PIDFILE=/usr/local/nagios/var/$NAME. lock

#chmod 755 nagios

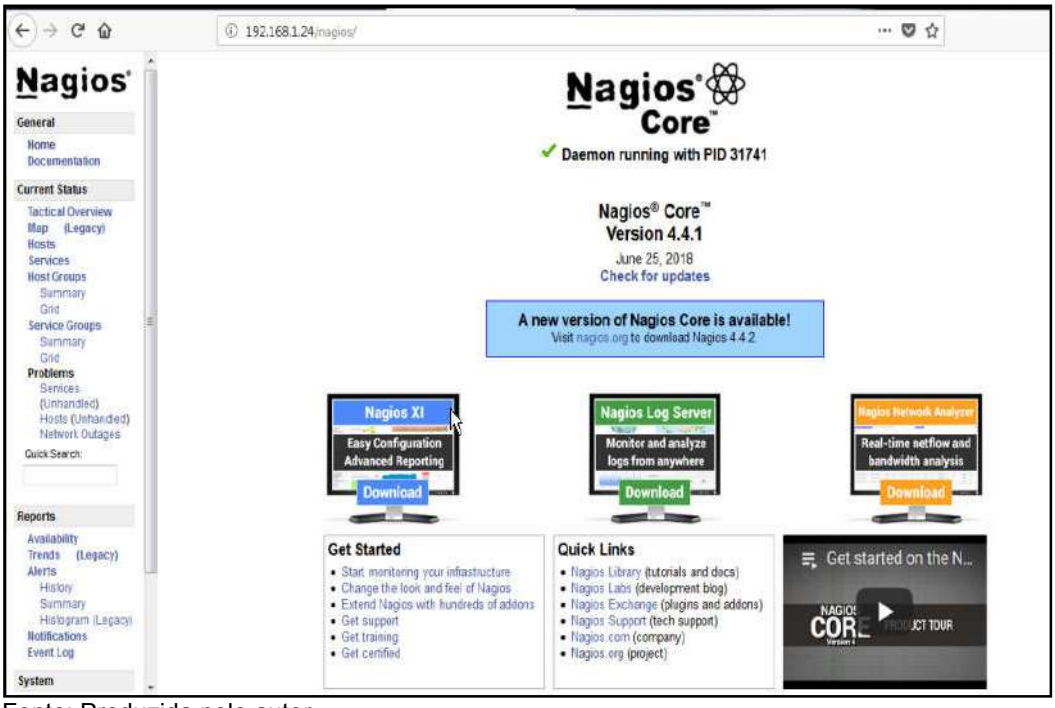
update-rc.d nagios defaults

/etc/init.d/nagios start

Acessar, conforme demonstra APÊNDICE M– Acesso ao Nagios Tela Inicial

http://IP/nagios/

Figura 18: Tela Inicial do Nagios



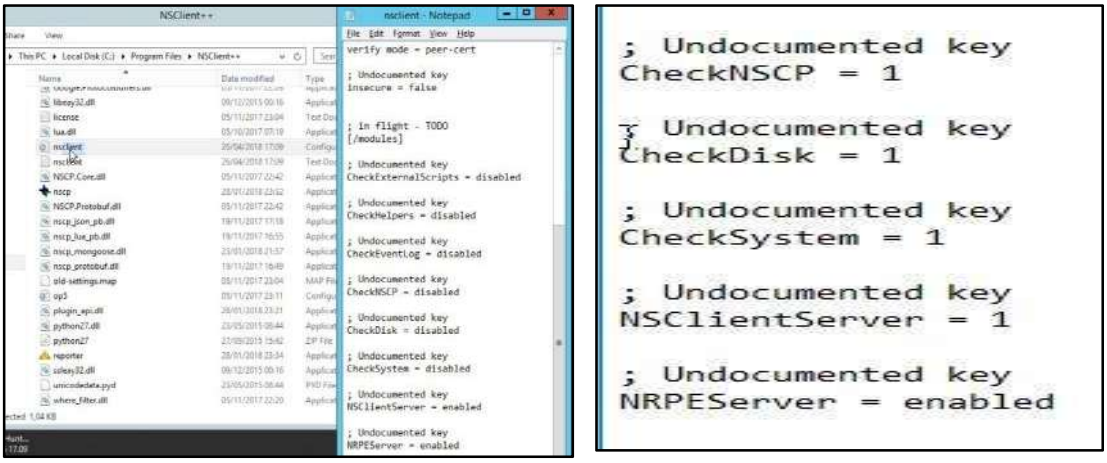
Fonte: Produzida pelo autor

A figura 18, acima apresenta tela de inicialização do nagios.

4.3Instalação NSClient - Desktop e Servidores

A instalaçãodo Agent NSClient foi realizada nos Servidores e desktop,que possuem o sistema operacional Windowspara realizar a checagem dos objetos como utilização da CPU, consumo de Memória, consumo de espaço nos Discos, Ping e também serviços como NSClient, Net-SNMP Agent, DHCPServer, DNS Server e S.O.S Backup. Onde o arquivo de configuração principal localiza-se no diretório“C:\Program Files\NSClient++\nsclient.ini”, necessita-se editar o modulo NSClientServer, digitando o número 1, para habilitar o monitoramento da CPU, Memória, Uso de Discos e Ping. Depois de realizado este procedimento, deve-se salvar o arquivo nsclient. ini e reiniciar oNSClient.

Figura 19: Agente NSClient



Fonte: Produzida pelo autor

A Figura 19 acima,a direta demonstra o arquivo nsclient.ini de configuração do agente no sistema operacional Windows 10 e Windows Server 2012r2 habilitado, para realizar da coleta do CPU, Discos, Ping, Memória e Serviços.

Os parâmetros do arquivo19 acima à direita, são módulos básicos nativos do NSClient, onde podemos habilitar os parâmetros digitando o número 1, para coletar e enviar informações ao gerente Servidor Nagios, neste caso foi habilitado NSClientServer para envio das informações ao gerente.

4.3.1Monitoramento de Desktop e Servidores com Agent NSClient

Para realizar o monitoramento de objetos relevantes nos Desktop e servidores, é necessário definir parâmetros para cada objeto, que se necessita monitorar, para capturar a informação do estado do objeto.

Abaixo serão demonstradas linhas de comando que definirão o monitoramento de objetos como: Uptime, CPU Load, Memory Usage , Unidade de disco e Serviços.

/usr/local/nagios/etc/objects/lwindows10.cfg

```
define host{
host_name                               Windows10
use                                     TemplateHostWindows
alias                                   Windows10
address                                 10.110.20.10
contact_groups                          admins
}
```

Os Parâmetros acima definem o host que iremos monitorar, informando o nome e o IP do equipamento em questão.

```
define service{
use                             TemplateService
host_name                       Windows10; Nome do host
service_description             PING-Disponibilidade Descricao do
Servico a ser monitorado para o host
check_command                   check_ping!100,20%!200,60%; Plugin e
Parametros
contact_groups                  admins
}
```

O parâmetro “check_ping” especifica-secondições, sejam elas: o número de pacotes em 100 milésimos de segundos definidos pelo numeral “100” ou 20% de perda de pacotes, neste caso serágerado o aviso (atenção).E por último se alcançar 200 milésimos de segundos definidos pelo numeral 200 ou 60% de perda de pacotes,gerará aviso crítico.

```
define service{
use                             TemplateService
host_name                       Windows10 ; Nome do host
service_description             HTTP      ; Descricao do Servico a ser
monitorado para o host
check_command                   check_tcpNP!80!1!2!; Plugin e Parametros
contact_groups                  admins
}
```

O parâmetro acima check_tcp, verifica a disponibilidade da porta 80, 1 warning e 2 crítico.

```
define service{
use                             TemplateService
host_name                       Windows10 ; Nome do host
service_description             Particao_C ;
check_command                   check_nt_disk!C!75!85!
contact_groups                  admins
}
```

O parâmetro acima “check_nt_disck” especifica-se condições, sejam elas: Se o uso da unidade C:\ chegar a 75 %, vai gerar alerta warning (atenção), e se chegar a 85 % um aviso de alerta de critico.

```
Define service{
use                             TemplateService
host_name                       Windows10 ; Nome do host
service_description             Memoria ; Descricao do Servico a ser
monitorado para o host
check_command                   check_nt_memuse!75!85! ; Plugin e
Parametros
contact_groups                  admins
}
```

O parâmetro “check_nt_memuse” especifica-se condições, sejam elas: O uso de memória no servidor chegar a 75 % de uso vai gerar alerta warning (atenção), e se chegar a 85 % um aviso de alerta de crítico.

```
define service{
use                             TemplateService
host_name                       Windows10 ; Nome do host
service_description             CPU ; Descricao do Servico a ser
monitorado para o host
check_command                   check_nt_cpuload ;CPULOAD!-l 5,80,90
Plugin e Parametros
contact_groups                  admins
}
```

O parâmetro acima check_nt_cpuload e a definição de serviço para monitorar a utilização da CPU no Windows, sejam elas: Gerar um alerta warning se a carga de CPU 5 minutos é 80% ou um aviso de alerta, se a carga de 5 minutos é de 90% ou maior (critico).

```
define service {
use                         TemplateService
host_name                   Windows10;
service_description         W3SVC
check_command               check_nt!SERVICESTATE!-d SHOWALL -l W3SVC
contact_groups              admins
}
```

O parâmetro acima check_nt!SERVICESTATE é a definição de serviço para monitorar o serviço se esta funcionando corretamente, se parar o serviço ira gerar um alerta (critico).

```
define service {
use                         TemplateService
host_name                   Windows10;
service_description         nscp NSCLIENT
check_command               check_nt!SERVICESTATE!-d SHOWALL -l nscp
contact_groups              admins
}
```

O parâmetro acima check_nt!SERVICESTATE é a definição de serviço para monitorar se esta UP ou DOWN, esse serviço nscp e a execução do nsclient do agente.

```
define service {
use                     TemplateService
host_name               WindowsServer2012R2DHCPDNS_snmpv3;
service_description     Active Directory Domain Services
check_command           check_nt!SERVICESTATE!-d SHOWALL -l NTDS
contact_groups          admins
}
```

O parâmetro acima check_nt!SERVICESTATE é a definição de serviço para monitorar o estado do objeto “NTDS”,Active Directory, gerar um alerta se o serviço for interrompido,(Critico).

```
define service {
use                     TemplateService
host_name               WindowsServer2012R2DHCPDNS_snmpv3
service_description     Net-SNMP Agent
check_command           check_nt!PROCSTATE!-d SHOWALL -lsnmpd.exe
contact_groups          admins
}
```

O parâmetro acima check_nt!SERVICESTATE é a definição de serviço para monitorar se esta up ou down, esse serviço “snmpd.exe” e a execução do “Net-SNMP Agent” do agente.

```
define service{
use                         TemplateService
host_name                   WindowsServer2012R2DHCPDNS_snmpv3
service_description         DNS_SERVER ; Descricao do Servico a ser
monitorado para o host
check_command               check_dns ; Plugin e Parametros
contact_groups              admins
}
```

O parâmetro acima check_dns é a definição de serviço para monitorar o estado do objeto “DNS_SERVER” gerar um alerta se o serviço for interrompido, (Critico).

```
define service {
use                     TemplateService
host_name               WindowsServer2012R2FILESERVER_snmpv3;
service_description     SOS BACKUP
check_command           check_nt!SERVICESTATE!-d SHOWALL -l
SOSBackup
contact_groups          admins
}
```

O parâmetro acima check_nt!SERVICESTATE é a definição de serviço para monitorar se esta up ou down, o serviço “SOS BACKUP”.

Após definirmos os parâmetros para todos os serviços que iremos monitorar, precisa habilitar o host, para que o Servidor Nagios reconheça o host cadastrado.

Editar arquivo nagios.cfg

nano /usr/local/nagios/etc/nagios.cfg

#Insira na primeira linha do arquivo

cfg_file=/usr/local/nagios/etc/objects/windows10.cfg

#Comando de teste, pra verificar se esta ok as configurações

/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

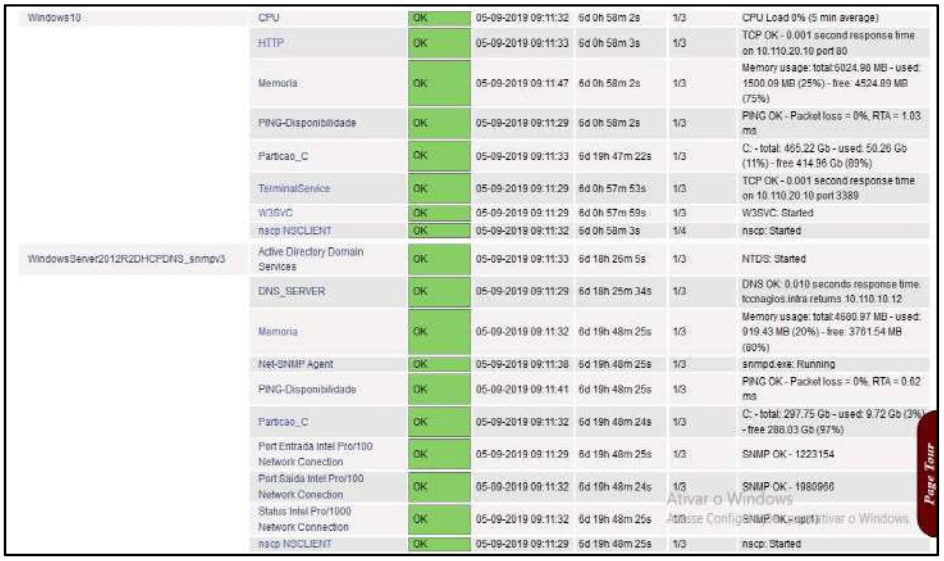
#Resultado deve ser semelhante a esse

Total Warnings: 0
Total Errors: 0
Caso o resultado não for semelhante, o parâmetro ira indicar o arquivo que o contém e ainda informa o número da linha com o erro.

#Reiniciar o serviço nagios
nagios:# /etc/init.d/nagios restart

Abaixo na figura 20, visualização via interface web do Nagios.

Figura 20: Painel de Monitoramento Nagios



Fonte: Produzida pelo autor

A figura 20 acima demonstra na tela inicial do Sistema de monitoramento nagios, o monitoramento dos ativos e serviços, Servidores e Desktop estão OK.

4.4 Monitoramento Impressora - Multifuncional Modelo 8912, SNMPV2

Para realizar o monitoramento de objetos da Impressora, é necessário definir parâmetros para cada objeto, que se necessita monitorar, para capturar a informação do estado do objeto.

Abaixo serão demonstradas linhas de comando que definirão o monitoramento de objetos como: Troca de Toner e disponibilidade da impressora

./usr/local/nagios/etc/objects/IMPRESSORA.cfg

```
define service{
use                             TemplateService
host_name                       IMPRESSORA
service_description             Toner ; Descricao do Servico a ser
monitorado para o host
check_command                   check_snmp_printer!public!CONSUM Black
Toner!30!20! ; Plugin e Parametros
contact_groups                  admins
}
```

Parâmetros acima definem o monitoramento do uso do toner se chegar a 30% atenção,se chegar a 20 crítico.

```
define service{
use                             TemplateService
host_name                       IMPRESSORA
service_description             PING-Disponibilidade ; Descricao do
Servico a ser monitorado para o host
check_command                   check_ping!100,20%!200,60% ; Plugin e
Parametros
contact_groups                  admins
}
```

O parâmetro “check_ping” especifica-se condições, sejam elas: o número de pacotes em 100 milésimos de segundos definidos pelo numeral “100” ou 20% de perda de pacotes, neste caso será gerado o aviso (atenção). E por último se alcançar 200 milésimos de segundos definidos pelo numeral 200 ou 60% de perda de pacotes, gerará aviso crítico.

Figura 21: Painel de Monitoramento Nagios

Fonte: Produzida pelo autor

A figura 21 acima, demonstra na tela inicial do Sistema de monitoramento nagios , que impressora e os serviços estão OK.

4.5.2 Monitoramento SNMPV2– Roteadores e Switchs

Monitoramento via SNMPV2, Status, Ping, UpTime e como foco as Interfaces de Entrada e Saída da rede

/usr/local/nagios/etc/objects/Switch.cfg

```
define host {

    use                     generic-switch
    host_name               linksys-srw224p
    alias                   Linksys SRW224P Switch
    address                 10.110.69.1
hostgroups              switches
}
```

Os Parâmetros acima definem o host que iremos monitorar, informando o nome e o IP do equipamento em questão.

```
define service {
use                     generic-service
host_name               Switch
service_description     PING
check_command           check_ping!200.0,20%!600.0,60%
```

O parâmetro “check_ping” especifica-secondições, sejam elas: o número de pacotes em 200 milésimos de segundos definidos pelo numeral “200” ou 20% de perda de pacotes, neste caso serágerado o aviso (atenção).E por último se alcançar 200 milésimos de segundos definidos pelo numeral 200 ou 60% de perda de pacotes,gerará aviso crítico.

```
define serv
ice {
use                     generic-service
host_name               Switch
service_description     Uptime
check_command           check_snmp!-C sw_tcc -o sysUpTime.0
}
```

Parâmetro acima se refere ao OID, para sysUpTime.0 operacional onde informa o tempo que está ligado.

```
define service {
use                      generic-service
host_name                Switch
service_description      Port 1 Link Entrada
check_command            check_snmp!-C sw_tcc -o ifInOctets.10001 -r
1 -m RFC1213-MIB
}
```

Parâmetro acima se refere ao OID, para o ifInOctets operacional da porta indicada, no caso porta 1(1001) no switch. Para taxa de bytes recebidos. A opção –r 1 informa ao plugin check_snmp para retornar um estado se “1” for encontrado no resultado SNMP (1 indica UP na porta) e CRITICAL senão for encontrado. O –m RFC1213-MIB refere-se para carregar apenas o RFC1213-MIB, em vez de cada MIB.

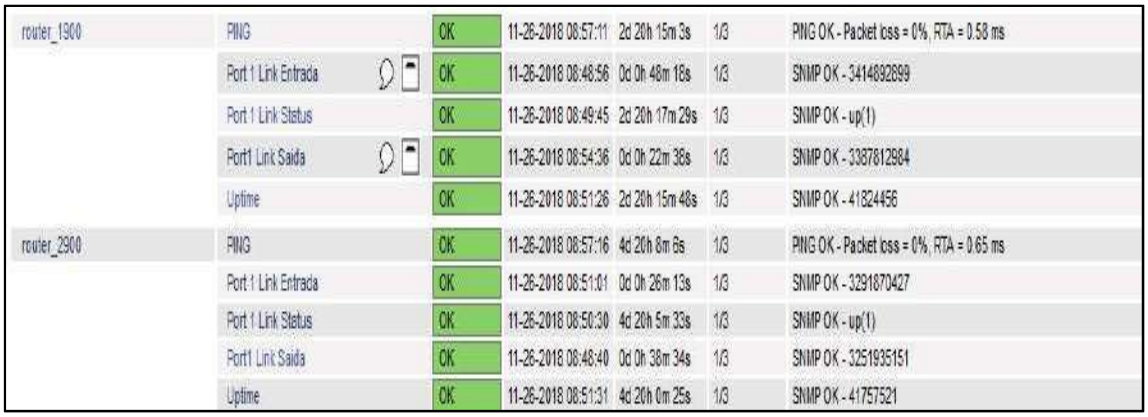
```
define service {
use                             generic-service
host_name                       Switch
service_description             Port 1 Link Saida
check_command                   check_snmp!-C sw_tcc -o ifOutOctets.10001 -
r 1 -m RFC1213-MIB
}
```

Parâmetro acima se refere ao OID, para o ifOutOctets operacional da porta indicada, no caso porta 1(1001) no switch. Para taxa de bytes enviados. A opção –r 1 informa ao plugin check_snmp para retornar um estado se “1” for encontrado no resultado SNMP (1 indica UP na porta) e CRITICAL senão for encontrado. O –m RFC1213-MIB refere-se para carregar apenas o RFC1213-MIB, em vez de cada MIB.

```
define service {
use                 generic-service
host_name           Switch
service_description     Port 1 Link Status
check_command           check_snmp!-C sw_tcc -o ifOperStatus.10001 -r 1 -m RFC1213-MIB
}
```

Parâmetro acima se refere ao OID, para o status operacional da porta indicada, no caso porta 1(1001) no switch. A opção –r 1 informa ao plugin check_snmp para retornar um estado se “1” for encontrado no resultado SNMP (1 indica UP na porta) e CRITICAL senão for encontrado. O –m RFC1213-MIB refere-se para carregar apenas o RFC1213-MIB, em vez de cada MIB.

Figura 22: Painel de Monitoramento Nagios - Roteadores e Switch



router_1900	PING	OK	11-26-2018 08:57:11	2d 20h 15m 3s	1/3	PING OK - Packet loss = 0%, RTA = 0.58 ms
	Port 1 Link Entrada	OK	11-26-2018 08:48:56	0d 0h 48m 18s	1/3	SNMP OK - 3414892899
	Port 1 Link Status	OK	11-26-2018 08:49:45	2d 20h 17m 29s	1/3	SNMP OK - up(1)
	Port1 Link Saida	OK	11-26-2018 08:54:36	0d 0h 22m 38s	1/3	SNMP OK - 3387812984
	Uptime	OK	11-26-2018 08:51:26	2d 20h 15m 48s	1/3	SNMP OK - 41824456
router_2900	PING	OK	11-26-2018 08:57:16	4d 20h 6m 6s	1/3	PING OK - Packet loss = 0%, RTA = 0.65 ms
	Port 1 Link Entrada	OK	11-26-2018 08:51:01	0d 0h 26m 13s	1/3	SNMP OK - 3291870427
	Port 1 Link Status	OK	11-26-2018 08:50:30	4d 20h 5m 33s	1/3	SNMP OK - up(1)
	Port1 Link Saida	OK	11-26-2018 08:46:40	0d 0h 38m 34s	1/3	SNMP OK - 3251935151
	Uptime	OK	11-26-2018 08:51:31	4d 20h 0m 25s	1/3	SNMP OK - 41757521

Fonte: Produzida pelo autor

A figura 22,acima, demonstra na tela inicial do Sistema de monitoramento nagios Roteadores e Switch estão OK.

4.6 Instalação SNMPV3 – Servidores DNS, DHCP e FILESERVER

- Instalar o **Activeperl** ,responsável por executar comandos predefinidos no host.

(http://www.activestate.com/Products/activeperl/download.mhtml),

Baixar o programa através desse link, após realizar o download, realizar a instalação padrão clicar em avançar até que a instalação esteja concluída.

- Instalar o Microsoft Visual C++ 2008 RedistributablePackage(x86), responsável por executar aplicativos que são desenvolvidos em linguagem C.

http://www.microsoft.com/downloads/details.aspx?familyid=9B2DA534-3E03-43918A4D-074B9F2BC1BF&displaylang=en)

Baixar o programa através desse link, após realizar o download, realizar a instalação padrão clicar em avançar até que a instalação esteja concluída.

- Instalação do Openssl de forma padrão, para o certificado de acesso.

http://www.slproweb.com/products/Win32OpenSSL.htm

Baixar o programa através desse link, após realizar o download, realizar a instalação padrão clicar em avançar até que a instalação esteja concluída.

OBS: A instalação deve ser selecionado os locais da DLL e escolher a opção “The Windows System Directory.

- Instalar Net-SNMP com suporte a SSL, responsável pela comunicação do protocolo SNMP com a ferramenta.

http://downloads.sourceforge.net/netsnmp/net-snmp-5.4.2-ssl1.win32.exe?modtime=1222072245&big_mirror=1

4.6.1 Monitoramentodas Interfaces SNMPV3 – Servidores DNS,DHCP e FILESERVER

Realizando monitoramento via snmpv3, Ping, Status e como foco as Interfaces da rede de entrada e saída.

```
define host{
host_name                              WindowsServer2012R2DNS_snmpv3
use                                    TemplateHostWindows
alias                                  WindowsServer2012R2DNS_snmpv3
address                                10.110.10.13
contact_groups                         admins

}
```

Os Parâmetros acima definem o host que iremos monitorar, informando o nome e o IP do equipamento em questão.

```
define service{
use                            TemplateService
host_name                      WindowsServer2012R2DNS_snmpv3; Nome do
host
service_description            PING-Disponibilidade ; Descricao do
Servico a ser monitorado para o host
check_command                  check_ping!100,20%!200,60% ; Plugin e
Parametros
contact_groups                 admins
}
```

O parâmetro “check_ping” especifica-secondições, sejam elas: o número de pacotes em 100 milésimos de segundos definidos pelo numeral “200” ou 20% de perda de pacotes, neste caso serágerado o aviso (atenção).E por último se alcançar 200 milésimos de segundos definidos pelo numeral 200 ou 60% de perda de pacotes,gerará aviso crítico.

```
define service{
use                            TemplateService
host_name                      WindowsServer2012R2DNS_snmpv3 ; Nome do
host
service_description            Status Intel Pro/1000 Network Connection
check_command             check_snmp!-o ifOperStatus.1 -P 3 -L
authNoPriv -U server_tcc -a MD5 -A "tcc@1234" -x DES -X "tcc@1234"
; Plugin e Parametros
contact_groups                 admins
}
```

Os Parâmetros acima definem o monitoramento do status da interface de rede do servidor DNS/DHCP, onde neste caso está sendo utilizado o protocolo SNMPv3, estão sendo definidos o OID do objeto a ser monitorado, usuário e senha de acesso SNMPv3.

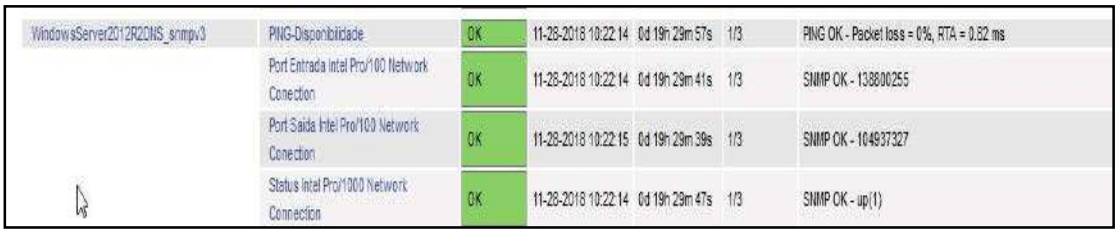
```
define service {
use                         TemplateService
host_name                   WindowsServer2012R2DNS_snmpv3
service_description         Port Entrada Intel Pro/100 Network
Conection
check_command               check_snmp!-o ifInOctets.12 -P 3 -L
authNoPriv -U server_tcc -a MD5 -A "tcc@1234" -x DES -X "tcc@1234"
; Plugin e Parametros
}
```

Os Parâmetros acima definem o monitoramento de bytes recebidos do objeto OID `ifInOctets` da interface de rede do servidor DNS/DHCP, onde neste caso está sendo monitorado numero de bytes que foram recebidos utilizado o protocolo SNMPv3, estão sendo definidos o OID do objeto a ser monitorado, usuário e senha de acesso SNMPv3.

```
define service {
use                             TemplateService
host_name                       WindowsServer2012R2DNS_snmpv3
service_description             Port Saida Intel Pro/100 Network
Conection
check_command                   check_snmp!-o ifOutOctets.12 -P 3 -L
authNoPriv -U server_tcc -a MD5 -A "tcc@1234" -x DES -X "tcc@1234"
; Plugin e Parametros
}
```

Os Parâmetros acima definem o monitoramento de bytes enviados do objeto OID `ifOutOctets` da interface de rede do servidor DNS/DHCP, onde neste caso está sendo monitorado numero de bytes que foram recebidos utilizado o protocolo SNMPv3, estão sendo definidos o OID do objeto a ser monitorado, usuário e senha de acesso SNMPv3.

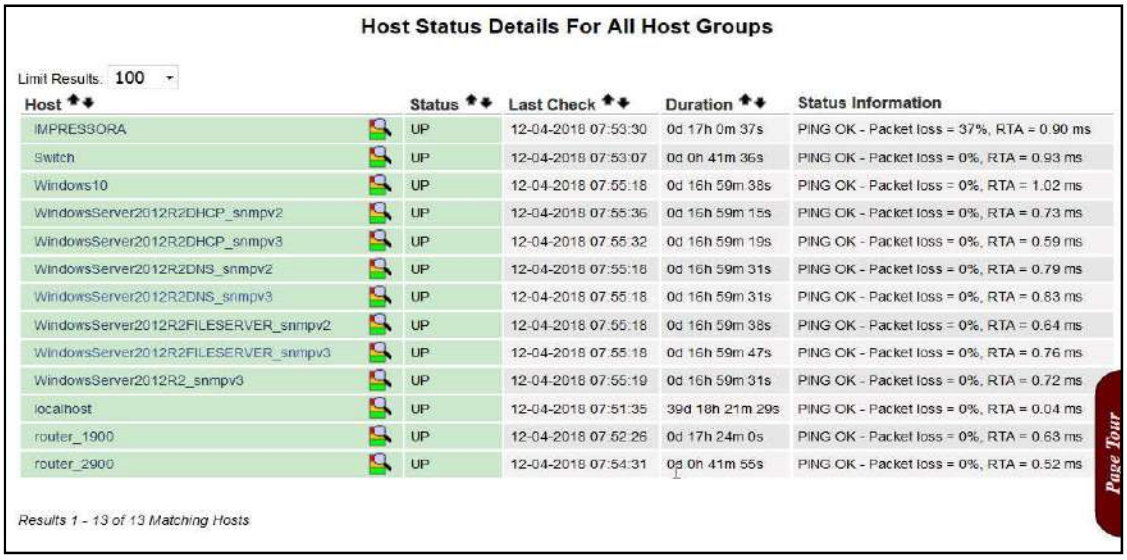
Figura 23: Painel de Monitoramento Nagios - SNMPV3



Fonte: Produzida pelo autor

A figura 23 acima demonstra na tela inicial do Sistema de monitoramento nagios, os Servidores e serviços estão OK,

Figura 24: Status dos hosts



Fonte: Produzida pelo autor

A figura 24 mostra status dos hosts tudo ok.

5 VALIDAÇÃO

Durante o projeto proposto, foram criados testes validando cada serviço e ativos de rede que estavam sendo monitorados. Os testes foram concluídos com êxito, conforme as Figuras 20 a 24 acima.

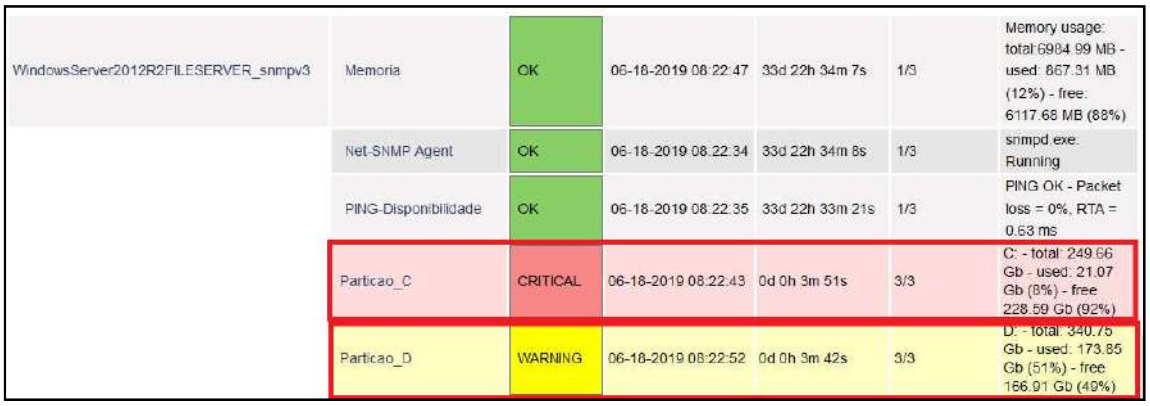
E através de testes realizados para verificar e certificar que o sistema de alertas programáveis e essencial no sistema de monitoramento, foi necessário simular anormalidade nos objetos notificando se o ativo ou serviço que está sendo monitorados e encontra UP, DONW ou WARNING.

Os testes realizados nos desktop e servidores para validação foi à verificação de objetos e serviços fundamentais no uso do equipamento, são eles: Quantidade de memória, Espaço em disco, Carga de CPU, Uptime do tempo ativo do Computador e serviços nos Servidores: como por exemplo, nsclient, DNSServer, Active Diretory, DHCPServer , Net-SNMP Agent e Serviço de Backup (S.O.S Backup), ondeforam definidos parâmetros, a cada objeto que está sendo monitorado.

Através dos parâmetros pré-definidos em cada objeto, o sistema emitira um alerta na tela de visualização do sistema de monitoramento Nagios na Web, para verificar se host ou serviço estão com alguma falha.

Conforme as figuras abaixo.

Figura 25: Interface Web Visualização do Estado dos Ativos e Serviços



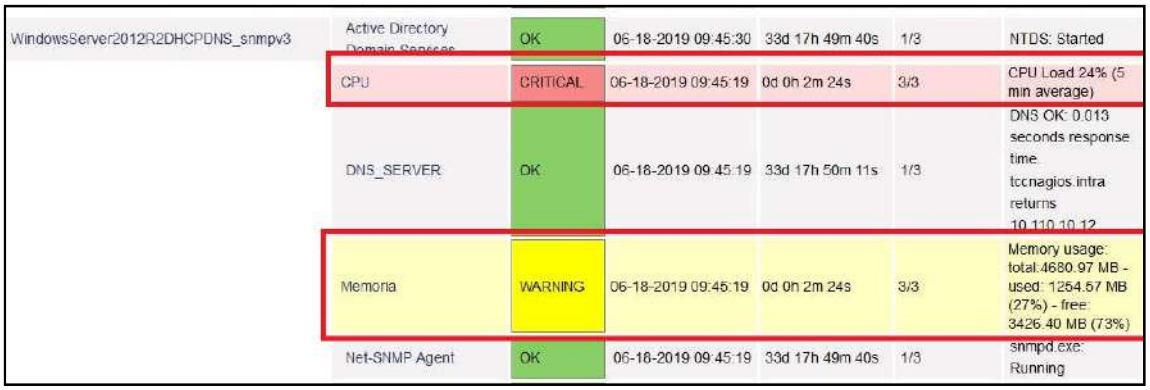
WindowsServer2012R2FILESERVER_snmpv3	Memoria	OK	06-18-2019 08:22:47	33d 22h 34m 7s	1/3	Memory usage: total:6984.99 MB - used: 867.31 MB (12%) - free: 6117.68 MB (88%)
	Net-SNMP Agent	OK	06-18-2019 08:22:34	33d 22h 34m 8s	1/3	snmpd.exe: Running
	PING-Disponibilidade	OK	06-18-2019 08:22:35	33d 22h 33m 21s	1/3	PING OK - Packet loss = 0%, RTA = 0.63 ms
	Particao_C	CRITICAL	06-18-2019 08:22:43	0d 0h 3m 51s	3/3	C: - total: 249.66 Gb - used: 21.07 Gb (8%) - free 228.59 Gb (92%)
	Particao_D	WARNING	06-18-2019 08:22:52	0d 0h 3m 42s	3/3	D: - total: 340.75 Gb - used: 173.85 Gb (51%) - free 166.91 Gb (49%)

Fonte: Produzida pelo autor

A figura25 acima demonstra notificações detalhadas e enviadas pelo sistema de monitoramento nagios, alertando, que o serviço esta com algum tipo de problema isso significa, que o objeto está acima do parâmetro configurado,como por exemplo: objeto da unidade de disco C:\ informa WARNING (atenção), e o tempo do alerta são de 3 minutos 51 segundos, objeto da unidade de disco D:\ informa CRITICAL (critico)e o tempo do alerta de 3 minutos e 42 segundos,senão for tratado pode virar um problema critico.Com base nesses alertas, o administrador pode tratá-lo da forma antecipada.

Através de um sistema de monitoramento e com essas informações dos objetos que foram configurados, podemos identificar o problema do host verificando se as unidades de disco esta com a capacidade cheia.

Figura 26: Interface Web Visualização do Estado dos Ativos e Serviços



WindowsServer2012R2DHCPDNS_snmpv3	Active Directory Domain Services	OK	06-18-2019 09:45:30	33d 17h 49m 40s	1/3	NTDS: Started
	CPU	CRITICAL	06-18-2019 09:45:19	0d 0h 2m 24s	3/3	CPU Load 24% (5 min average)
	DNS_SERVER	OK	06-18-2019 09:45:19	33d 17h 50m 11s	1/3	DNS OK: 0.013 seconds response time. tccnagios.intra returns 10.110.10.12
	Memoria	WARNING	06-18-2019 09:45:19	0d 0h 2m 24s	3/3	Memory usage: total:4680.97 MB - used: 1254.57 MB (27%) - free: 3426.40 MB (73%)
	Net-SNMP Agent	OK	06-18-2019 09:45:19	33d 17h 49m 40s	1/3	snmpd.exe: Running

Fonte: Produzida pelo autor

A figura 26 demonstra mais alertas na tela de monitoramento, onde esses objetos, CPULoad e a memória do Windows Server2012,estão apresentando alguma anomalia ”WARNING” e “CRITICAL, o alerta da CPU apresenta 2 minutos e 24 segundos alertando como CRITICALe a MEMORIA de 2 minutos de 24 segundos alertando WARNING.

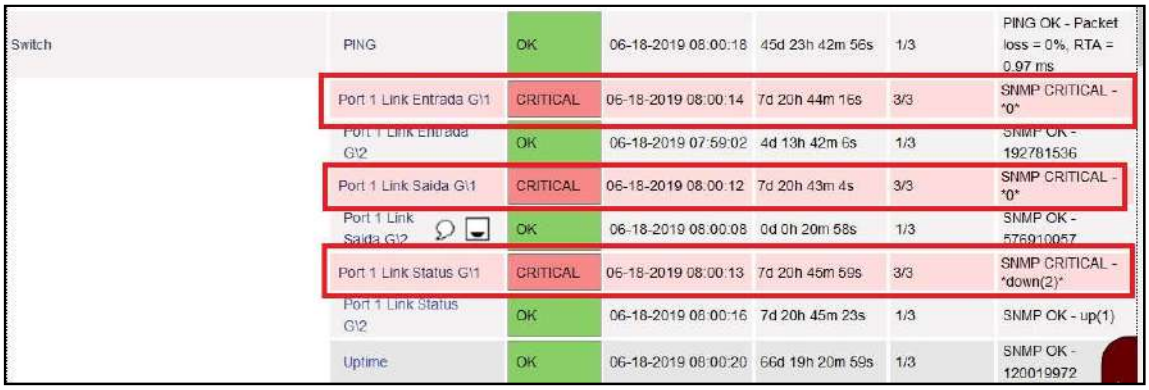
Através de um sistema de monitoramento e com essas informações podemos identificar o problema. Verificando consumo do computador e a capacidade de consumo da memória do computador tomando as medidas cabíveis.

Figura 27: Interface Web Visualização do Estado dos Ativos e Serviços

Fonte: Produzida pelo autor

A figura 27acima demonstra os objetos do ROUTER 2900 em monitoramento, como Ping, tráfego de entrada de pacotes da interface de rede, tráfego de saída de pacotes da interface de rede e o Uptime da interface de rede do referido equipamento onde estão apresentando alertas CRITICAL, devido à indisponibilidade dos serviços.

Figura 28: Interface Web Visualização do Estado dos Ativos e Serviços



Switch	PING	OK	06-18-2019 08:00:18	45d 23h 42m 56s	1/3	PING OK - Packet loss = 0%, RTA = 0.97 ms
	Port 1 Link Entrada G\1	CRITICAL	06-18-2019 08:00:14	7d 20h 44m 16s	3/3	SNMP CRITICAL - *0*
	Port 1 Link Entrada G\2	OK	06-18-2019 07:59:02	4d 13h 42m 6s	1/3	SNMP OK - 192781536
	Port 1 Link Saida G\1	CRITICAL	06-18-2019 08:00:12	7d 20h 43m 4s	3/3	SNMP CRITICAL - *0*
	Port 1 Link Saida G\2	OK	06-18-2019 08:00:08	0d 0h 20m 58s	1/3	SNMP OK - 576910057
	Port 1 Link Status G\1	CRITICAL	06-18-2019 08:00:13	7d 20h 45m 59s	3/3	SNMP CRITICAL - *down(2)*
	Port 1 Link Status G\2	OK	06-18-2019 08:00:16	7d 20h 45m 23s	1/3	SNMP OK - up(1)
	Uptime	OK	06-18-2019 08:00:20	66d 19h 20m 59s	1/3	SNMP OK - 120019972

Fonte: Produzida pelo autor

A figura 28 acima demonstra monitoramento do ativo de redeSWITCH, onde os objetos que estão sendo monitorados estão apresentando algum problema,os objetos como Port 1 Link Entrada G/1, Port 1 Link Saida G/1 e Port 1 Link Status G/1, esta apresentando alertas CRITICAL.

Nota-se alertas críticos referente ao ping por não estar respondendo, o tráfego de entrada da interface gigabitEthernet por não estar recebendo pacotes, o status da interface de rede gigabitEthernet por estar desativada, o tráfego de saída da interface gigabitEthernet por não estar transmitindo pacotes e a indisponibilidade do equipamento.

Com a utilização do Nagios será possível realizar o monitoramento dos objetos mencionados acima, agindo de forma proativa, identificando possíveis problemasna rede, conforme as figura 27 e 28, por exemplo, demonstrado um possível problema na interface de rede.

Figura 29: Interface Web Visualização Serviço de DNS SERVER

WindowsServer2012R2DHCPDNS_snmpv3	Active Directory Domain Services	OK	06-20-2019 15:09:31	0d 0h 9m 25s	1/3	NTDS: Started
	CPU	OK	06-20-2019 15:09:20	0d 0h 9m 36s	1/3	CPU Load 13% (5 min average)
	DHCPSERVER	UNKNOWN	06-20-2019 15:09:33	3659d 18h 22m 45s	3/3	Usage:
	DNS_SERVER	CRITICAL	06-20-2019 15:08:43	0d 0h 1m 13s	1/3	CRITICAL - Plugin timed out while executing system call
	ENTRADA Intel Pro/1000 Network Connection	OK	06-20-2019 15:09:43	0d 0h 10m 13s	1/3	SNMP OK - 4072490
	Memoria	OK	06-20-2019 15:09:31	0d 0h 9m 25s	1/3	Memory usage: total:3518.46 MB - used: 969.02 MB (28%) - free: 2549.44 MB (72%)
	Net-SNMP Agent	OK	06-20-2019 15:09:31	0d 0h 9m 25s	1/3	snmpd.exe: Running

Fonte: Produzida pelo autor

A figura 29 acima demonstra monitoramento do serviço DNS_SERVER, aonde informa com detalhes na tela de monitoramento do Nagios, queesta CRITICAL há 1 minuto e 13 segundos.

Figura 30: Interface Web Visualização Serviço de Backup

Port Entrada Intel Pro/100 Network Conection	OK	06-18-2019 12:37:13	34d 2h 49m 1s	1/3	SNMP OK - 1039919173
Port Saida Intel Pro/100 Network Conection	OK	06-18-2019 12:37:19	34d 2h 48m 10s	1/3	SNMP OK - 366170216
SOS BACKUP	CRITICAL	06-18-2019 12:37:27	0d 0h 9m 46s	3/3	SOSBackup: Stopped
Status Intel Pro/1000 Network Connection	OK	06-18-2019 12:37:13	34d 2h 48m 5s	1/3	SNMP OK - u
nscp NSCLIENT	OK	06-18-2019 12:37:31	34d 2h 48m 0s	1/3	nscp: Started

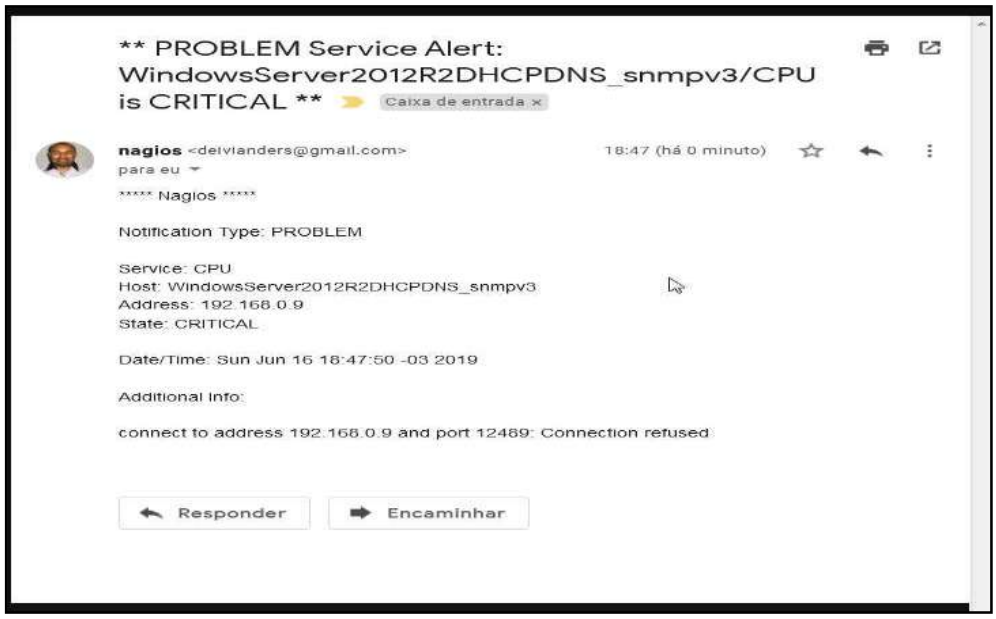
Fonte: Produzida pelo autor

A figura 30acima demonstra detalhadamente a indisponibilidade de um serviço importante, objeto S.O.S Backup parado a 9 minutos e 46 segundos .

Além de gerar alertas, o sistema de monitoramento nagios nos propõe a notificação por email quando um serviço estiver com problema.

Conforme a figura abaixo:

Figura 31: Notificação por e-mail CPU

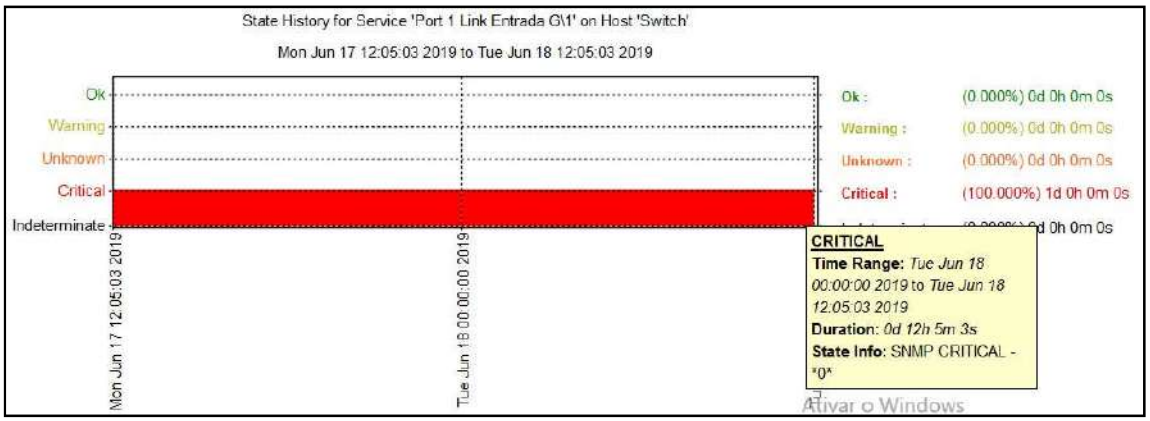


Fonte: Produzida pelo autor

Outro recurso do sistema de monitoramento nagios e a possibilidade de tirar relatório de históricos do estado de cada objeto podendo assim gerar as notificações por dias, semanas ou mês e se necessário gerar gráficos.

Como por exemplo, a figura 32 abaixo e um relatório de período de tempo do serviço “PING do router_ 2900”, onde nos informa a indisponibilidade e tempo que ficou parado o serviço.

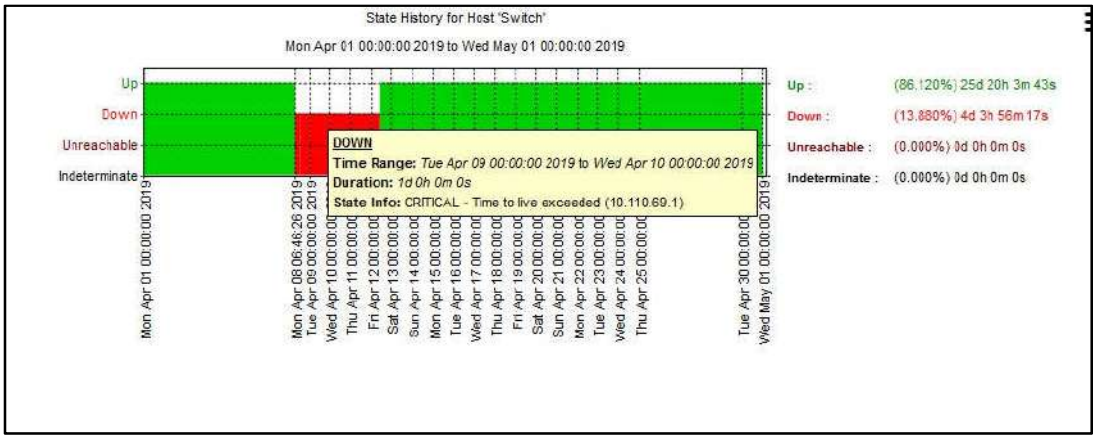
Figura 32: Histórico do host Roteador 2900



Fonte: Produzida pelo autor

A figura 32 demonstra o alerta da indisponibilidade do Router 2900, informando detalhadamente quanto tempo ficou com problema o ativo de rede 12horas e 5 minutos e 3 segundos.

Figura 33:Histórico do Switch

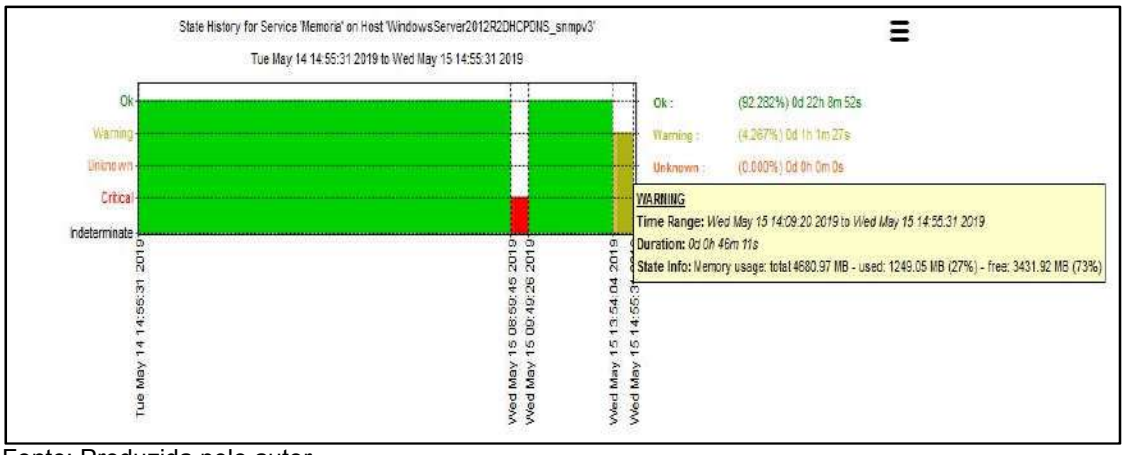


Fonte: Produzida pelo autor

A figura 33 demonstra histórico do ativo de rede com as informações detalhadas da indisponibilidade do equipamento Switch, entre o dia 08 a 12. Informando que o ativo da rede ficou em alerta 4 dias 3 hora 56 minutos e dezessete segundos.

Outro exemplo demonstrado abaixo é históricos de alertas da memória onde se demonstra períodos de indisponibilidade do referido objeto .

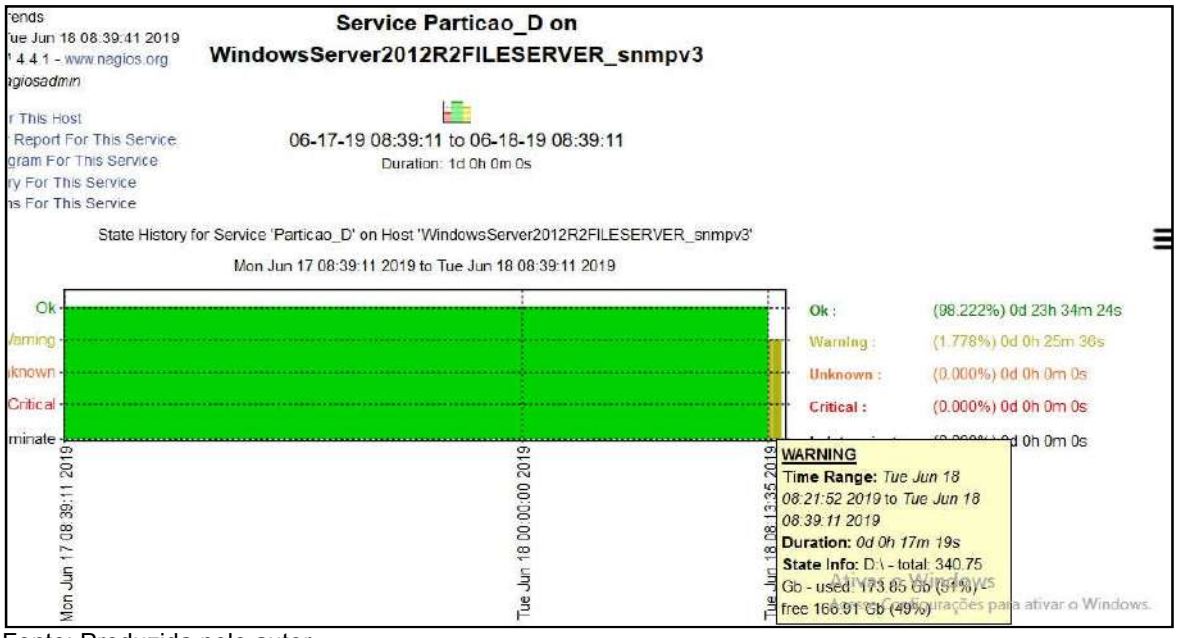
Figura 34: Histórico da Memória



Fonte: Produzida pelo autor

A figura 34 demonstram alertas que ocorrem entre dos dias 14 a 15 de junho a cor de vermelho o tempo 10m 18s que ficou CRITICAL e de amarelo 46 minutos e 11 segundos WARNING.

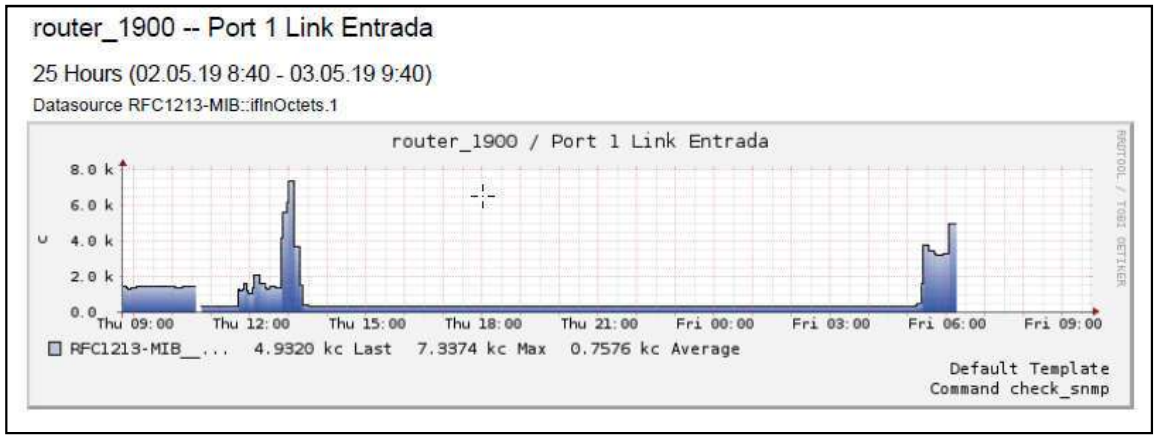
Figura 35: Histórico da Partição da Unidade D:\



Fonte: Produzida pelo autor

A figura 35acima ilustra com detalhes o histórico da partição D:\ notificando, que o serviço esta em alerta a 17 minutos 19 segundos (Warning)da partição D:\.

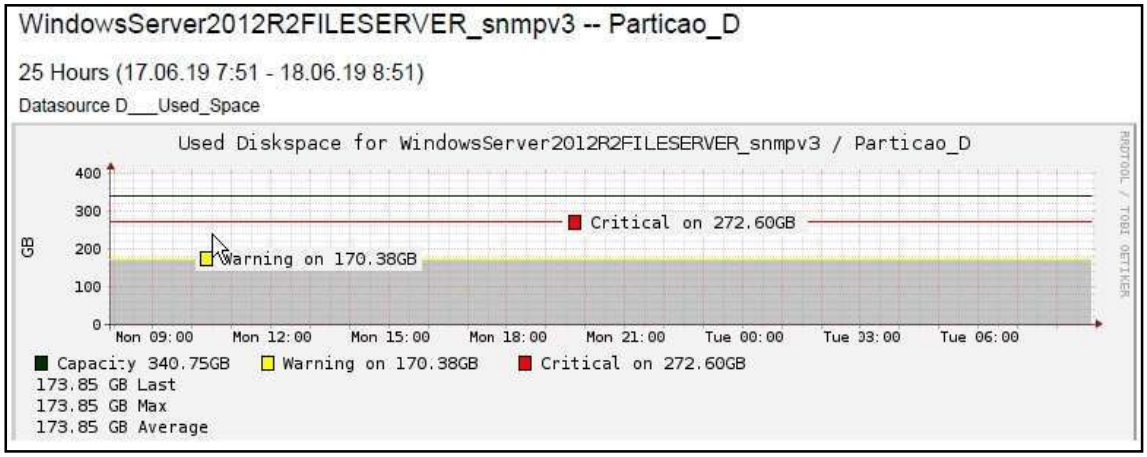
Figura 36: Gráfico do Serviço do ifInOctets.1do Roteador 1900



Fonte: Produzida pelo autor

A figura 36acima demonstra uma analise automática realizada pelo sistema de integração do nagios PNP4 de 25 horas, aonde indica os dados de desempenho da interface do router 1900, detalhando um aumento na entrada de dados por volta das 12:00, do objeto porta 1 Link do router 1900.

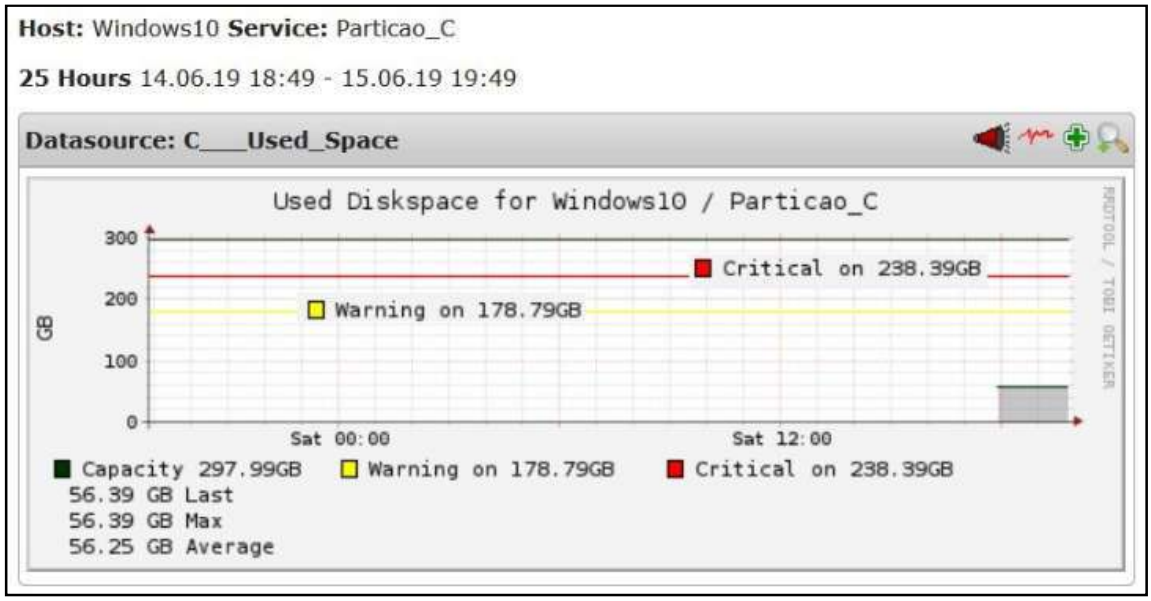
Figura 37: Gráfico da unidade de DISCO D:\ WINDOWS SERVER2012FILESERVER



Fonte: Produzida pelo autor

A figura 37 acima,mostracom detalhes o nível de consumo da unidade d:\, onde indica que o total de consumo foi de 173,85.

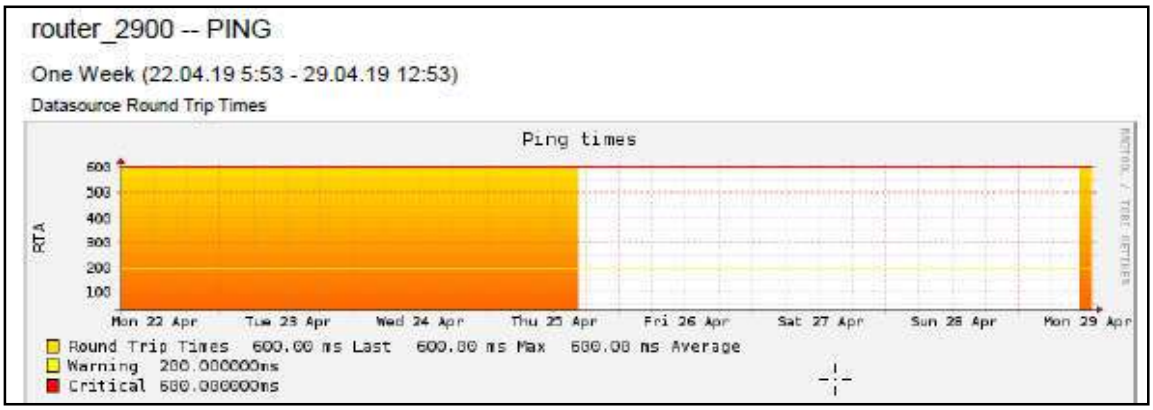
Figura 38: Gráfico da unidade de DISCO C:\ WINDOWS SERVER2012FILESERVER



Fonte: Produzida pelo autor

A figura 38 acima, mostra com detalhes o nível de consumo da unidade C:\, onde indica que o total de consumo foi de 56,39. Indicando que o consumo esta ok

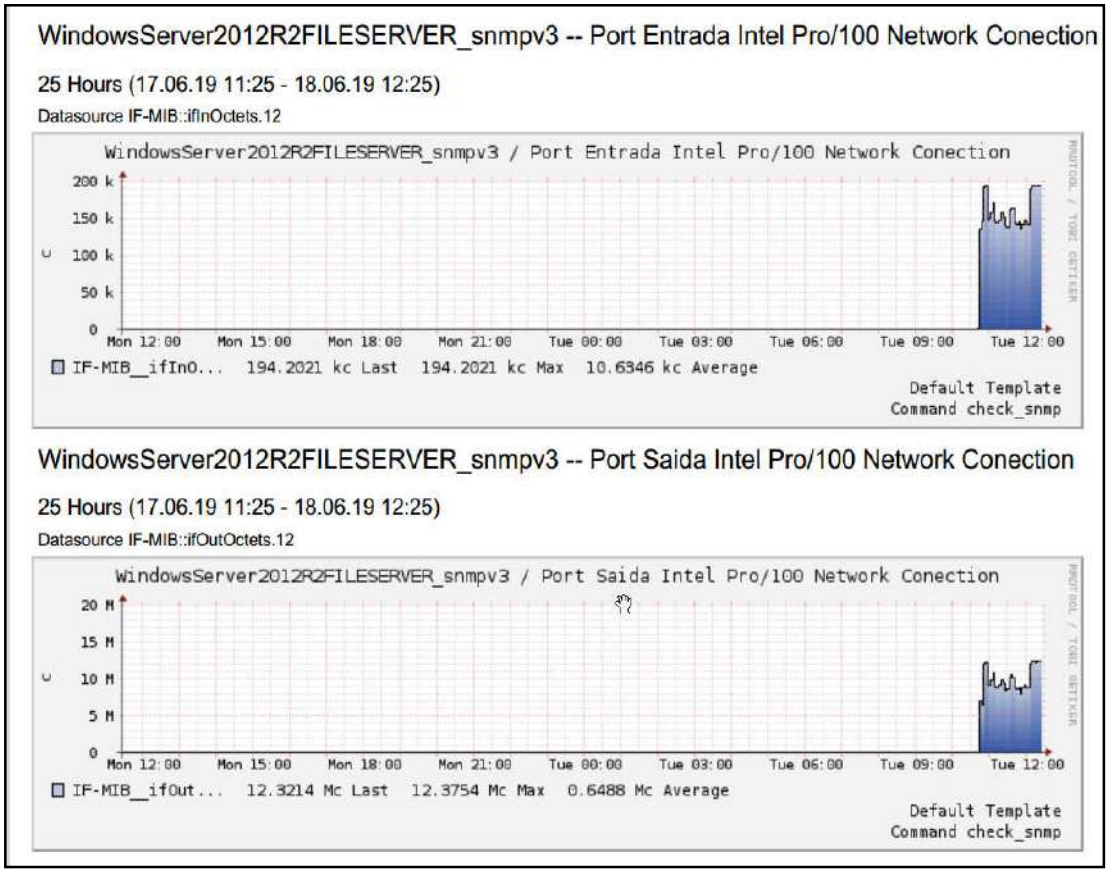
Figura 39: Gráfico Roteador 2900



Fonte: Produzida pelo autor

A figura 39 acima, mostra com detalhes o nível de trafego de dados informando que o Round Trip Times esta em 600 milesimos de segundos nos dias 22 a 25 de abril.

Figura 40: Gráfico Interface da Rede

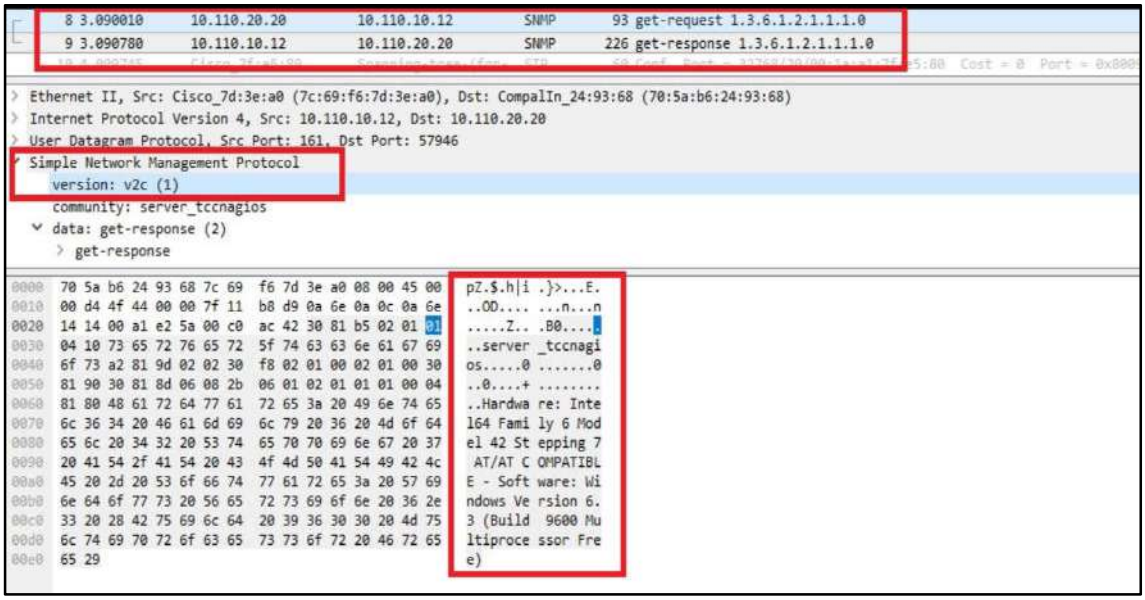


Fonte: Produzida pelo autor

A figura 40 acima demonstra graficamente com detalhes os níveis de tráfegos de entradas e de saída da interface do Servidorwindowsserver2012FILESERVER, aonde o fluxo maior por volta das 12h00min foi de saída obtendo Max 12, 3214mb enquanto a de entrada obteve 194.2021k.

Por fim demonstra-se nas figuras abaixo, um teste realizado na captura de dados na rede obtidos através do software wireshark.Podemos observar que os dados trafegados estão utilizando o protocolo SNMPv3, onde no servidor DNS foram utilizados os protocolos SNMPv2 e SNMPv3 a fim de realização de testes.

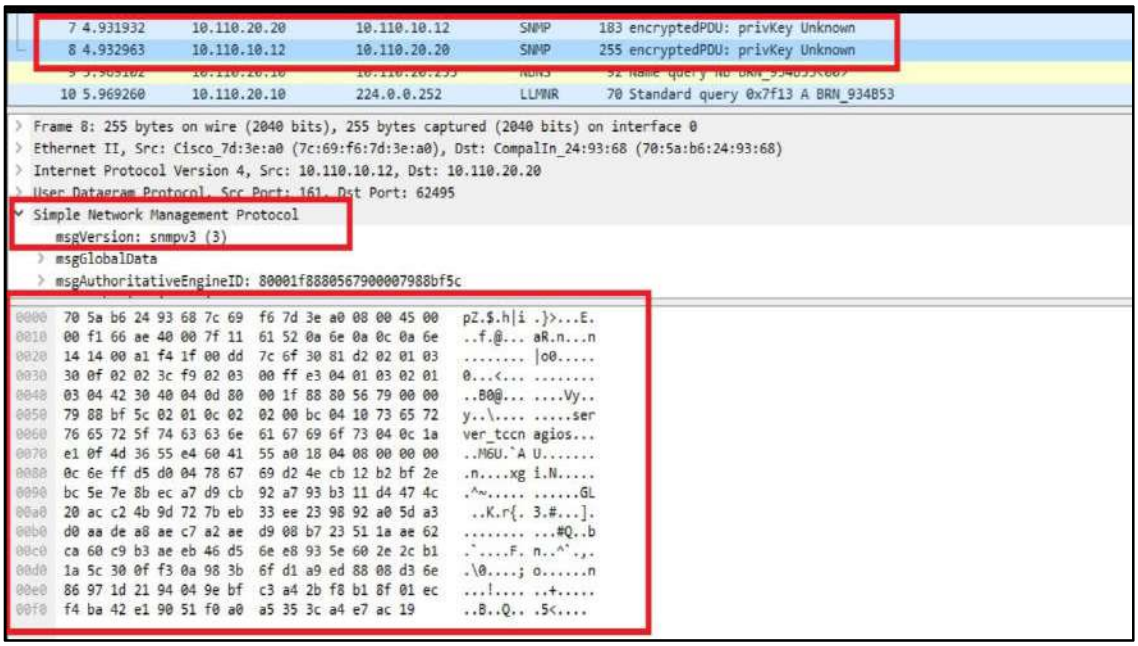
Figura 41: Captura Protocolo snmpv2



Fonte: Produzida pelo autor

A figura 40 acima demonstra uma captura da informação da OID(sysDescr.0), em snmpv2,Valor textual contendo a descrição da interface. Este texto pode conter informações diversas (tal qual o nome do fabricante, do produto ou versão de interfaces de hardware). Conforme destacado na imagem de vermelho.

Figura 42: Captura Protocolo snmpv3



Fonte: Produzida pelo autor

A figura 41 acima demonstra uma captura da informação da OID(sysDescr.0), Aonde as informações estão criptografadas e autenticadas ao usar o protocolo snmpv3. Conforme destacado na imagem de vermelho.

Assim demonstram as imagens acima as capturas de dados realizadas pelo wireshark,onde as informações serão criptografadas e autenticadas ao usar o protocolo snmpv3, conforme destacado nas imagens 41acima, enquanto o protocolo snmpv2 destacado na imagem 40não apresenta criptografia para segurança dos dados, podendo assim deixar uma brecha para coleta de informações sigilosas por algum invasor.

Finalmente, cada vez que um erro é encontrado pelo sistema de monitoramento Nagios, uma ação proativa será realizada sem que o usuário perceba.

6 CONCLUSÃO

Objetivo do projeto proposto de implementação de um sistema de monitoramento em um ambiente educacional utilizando a ferramenta Nagios, foi alcançado com êxito, mas com algumas ressalvas.

- Primeiro ponto positivo foi demonstrar que um sistema de monitoramento tem a capacidade de estar informando a disponibilidade e o desempenho de cada objeto programado a monitorar, verificando falhas ou anomalias.
- Segundo ponto positivo foi a criação do cenário no projeto, simulando um ambiente educacional, onde foi possível a instalação do Servidor Nagios (gerente), para coletar as informações dos objetos, que estavam sendo monitorados através do agente NSClient e o protocolo de gerenciamento SNMP, que foram instalados nos Servidores, desktop, Roteadores e Switch.
- Terceiro ponto positivo, foi utilizar a interface web do nagios para realizar as coletas de informações dos ativos de rede e serviços no cenário proposto, verificando se os objetos monitorados apresentam alguma anomalia, como Memória, espaço em disco, CPU load, UpTime, Serviço do DNSServer, Serviço do Agente NSClient, Serviço

Active directory, Serviço de Backup e o monitoramento do fluxo de trafego de dados e falhas nos dispositivo de rede,informando e notificando quando houver alguma disponibilidade ou erro no item monitorado .

- Quarto ponto positivo, foi à implementação do protocolo snmpv3, para que seja mais segura os dados trafegados nas interfaces, autenticando e criptografando as informações.

Através dos resultados obtidos observou-se, que é de extrema importância um sistema de monitoramento que possa identificar problemas em tempo hábil, porque se a rede não for monitorada o problema só será identificado através do usuário ou quando parar o serviço.

Com objetivo alcançado, foi possível adquirir conhecimentos obre a ferramenta através de Documentação disponibilizada no próprio site do Nagios.

Através do estudo realizado para o projeto foi possível adquirir conhecimento nos protocolos de monitoramento como snmpv2 e snmpv3 e o agente nsclient, desenvolvido pelo nagios.

- Ponto negativo não foi possível realizar o monitoramento do Serviço DHCP, por apresentar erro de comando nos parâmetros.
- Recomendações para trabalhos futuros monitoramento de outros serviços nos servidores como forma de controle.

7 CRONOGRAMA

Tabela 3: Cronograma

Atividades	**Meses**									
	ANO 2017				ANO 2019					
	Mar	Abr	Mai	Jun	Fev	Marc	Abril	Maio	Jun	Julh
Escolha do assunto do projeto	X									
Elaboração da estrutura do projeto	X									
Seleção e leitura das obras para elaboração do projeto		X	X							
Elaboração dos objetivos, delimitação do tema e definição do problema		X	X							
Elaboração da pesquisa bibliográfica e documental do projeto			X	X	X					
Revisão final do texto e elaboração da introdução e conclusão		X	X	X		X	X	X	X	X
Data limite de entrega do Projeto de Estágio				X	X	X	X	X	X	X

8 REFERÊNCIAS BIBLIOGRÀFICA

Admin, **Entendendo a estrutura do Nagios** Disponível em: http://nagios-br.com/entendendo-a-estrutura-do-nagios Acesso em: março 2018.

Behrouz A. Forouzan, **COMUNICAÇÃO DE DADOS E REDES DE COMPUTADORES**, Quarta Edição, AMGH Editora LTDA Ano 2010.

BRISA, **SOCIEDADE BRASILEIRA PARA INTERCONEXÃO DE SISTEMAS ABERTOS**, Uma Abordagem de Sistemas Abertos, Ano 1993.

Chris Fry and Martin Nystrom, **Security Monitoring,**February 2009 First Edition.

CHIES RAFAEL, **Não, clientes (proxies) para serviços JAX-WS não são thread safe pela spec !** Disponível em: https://blogdorafaelchies.wordpress.com/ Acesso em: março 2018

CHRIS SANDERS, **PRATICAL PACKET ANALYSIS,**using wireshark to solve real-world network problems, Ano 2010.

Carlos Eduardo do Val, **ubuntu, Guia do Iniciante,** 1º Edição 2010.

David Josephsen, **Building A Monitoring Infrastructure With Nagios,**Ano 2007.

DOUGLAS E.COMER, **Interligação de Redes com TCP/IP,** Princípios, protocolos e arquitetura, Volume 1 6° Edição 2014.

Douglas R. Mauro E Kevin J. Schmidt, **Essential SNMP, Edition 2**, Ano 2005.

EVI NEMETH / GARTH SNYDER / TRET.RHEIN, **MANUAL COMPLETO DO LINUX, Guia do administrador,** SEGUNDA EDIÇÃO 2007.

Ethan Galstad, **Nagios Core Version 3.x Documentation,** Copyright © 1999-2009.

Herrero Hector, **nagios-monitorizando-nrpe,** Disponível em: http://www.bujarra.com/nagios-monitorizando-nrpe/?lang=en Acesso em: março 2018

Kurose, Ross, **Computer Networking, A Top-Down Approach, sixth edition** Ano 2013.

Kurose, James F, **Redes de computadores e a Internet: uma abordagem top-down**, 3. Edição, São Paulo.

Max Schubert , Derrick, JonathanGines, Andrew Hay, John Strand,**Nagios 3 Enterprise Network Monitoring Including Plug-Ins and Hardware Devices**.Ano 2008.

Nagios Core | **Nagios** Disponível em: http://www.nagios.org Acesso em : março 2018

Nagios Core | **Nagios – Brazilian Community,** Disponível em: http://nagios-br.com/nagios-coreAcesso em: março 2018

Nagios Core | **Nagios – Brazilian Community,**Configurando o Nagios pela primeira vez Disponível em: http://nagios-br.com/configurando-o-nagios-pela-primeira-vez-para-iniciantes Acesso em: março 2017

Nagios Core | **Nagios – Brazilian Community,**Fórum oficial em português do Nagios em: http://nagios-br.com/forum-oficial-em-portugues-do-nagios-respondendo-suas-duvidas Acesso em: março 2017

Nagios Core | **Nagios – Brazilian Community,**Entendendo e instalando o plugin nrpe Disponível em: http://nagios-br.com/entendendo-e-instalando-o-plugin-nrpe Acesso em: março 2018

NSCLIENT++, **Welcome to NSCLIENT++**, Disponível em: https://www.nsclient.org/ Acesso em: março 2018

Tom Ryder, **Nagios Core Administration Cookbook**, First published: January 2013.

Olivier Bonaventure, **Computer Networking: Principles Protocols and Practice**, October 30,2011.

Oliviera Esdras, 2015 **Modelo TMN: SNMP x OSI,**http://www.teleco.com.br/tutoriais/tutorialmodelotmn/pagina_2.asp, Acesso em: março 2017.

OLIVEIRA, Marcos Henrique de. **Nagios Monitorando Redes Corporativas**, Editora ciência moderna 2014, Rio de Janeiro.

Pinheiro Ricardo, 2015 **Mundotibrasil: O PROTOCOLO SNMP,** https://www.mundotibrasil.com.br/o-protocolo-snmp/ Acesso em: março 2017.

Richard Bejtlich, **The Practice of Network Security Monitoring**, Ano 2013.

STALLINGS, W. **SNMP, SNMPv2, SNMPv3 and RMON1 and 2.**Terceira Edição. Editora Addison-Wesley, 1998.

STALLINGS, William. **Arquitetura e organização de computadores,** 8 ed São Paulo 2010.

TANENBAUM, Andrew S. **Redes de computadores**, 4. Ed. Americana. São Paulo:

TANENBAUM, Andrew S. **Redes de computadores**, 5. Ed. Americana. São Paulo: Pearson Prentice Hall, 2011.

TEIXEIRA, Ramos. **Redes de Computadores, serviços, administração e segurança**. 1ª edição.

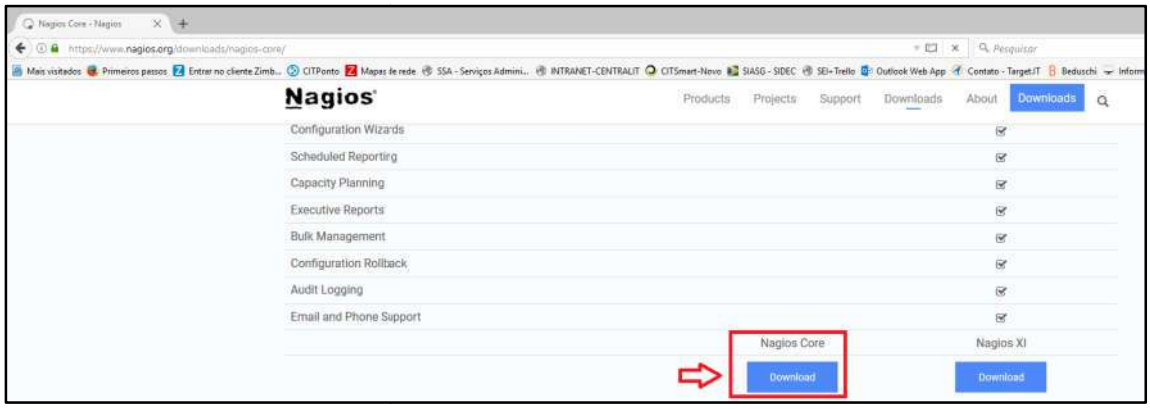
Wojciech Kocjan. **Learning Nagios 3.0**, First published: October 2008.

Wojciech Kocjan. **Learning Nagios 4.0**, Second Edition: March 2014.

Wolfgang Barth. **Nagios System and Network Monitoring**, Ano 2006.

9 APÊNDICES

9.1 APÊNDICE A - Download do Nagios.



9.2 APÊNDICE B - Download do Nagios Core

```
root@ubuntu:/home/nagios# wget https://assets.nagios.com/downloads/nagioscore/re
leases/nagios-4.4.1.tar.gz
--2019-07-23 02:45:08--  https://assets.nagios.com/downloads/nagioscore/releases
/nagios-4.4.1.tar.gz
Resolvendo assets.nagios.com (assets.nagios.com)... 72.14.181.71, 2600:3c00::f03
c:91ff:fedf:b821
Conectando-se a assets.nagios.com (assets.nagios.com)|72.14.181.71|:443... conec
tado.
A requisiÃ§Ã£o HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: 11296403 (11M) [application/x-gzip]
Salvando em: ânagios-4.4.1.tar.gz.1â

100%[=====================================>] 11.296.403  4,41MB/s    em 2,4s

2019-07-23 02:45:11 (4,41 MB/s) - ânagios-4.4.1.tar.gz.1â

root@ubuntu:/home/nagios#
```

9.3 APÊNDICE C - Download Plug-ins

```
root@ubuntu:/home/nagios# wget https://nagios-plugins.org/download/nagios-plugin
s-2.2.1.tar.gz
--2019-07-23 02:49:35--  https://nagios-plugins.org/download/nagios-plugins-2.2.
1.tar.gz
Resolvendo nagios-plugins.org (nagios-plugins.org)... 72.14.186.43
Conectando-se a nagios-plugins.org (nagios-plugins.org)|72.14.186.43|:443... con
ectado.
A requisiÃ§Ã£o HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: 2728818 (2,6M) [application/x-gzip]
Salvando em: ânagios-plugins-2.2.1.tar.gzâ

100%[=====================================>] 2.728.818   1,90MB/s    em 1,4s

2019-07-23 02:49:39 (1,90 MB/s) - ânagios-plugins-2.2.1.tar.gzâ

root@ubuntu:/home/nagios#
```

APÊNDICE D – Descompactar arquivos

```
root@ubuntu:/home/nagios# tar xzf nagios-4.4.1.tar.gz
root@ubuntu:/home/nagios# tar xzf nagios-plugins-2.2.1.tar.gz
root@ubuntu:/home/nagios# ls
dead.letter          nagios-4.4.1.tar.gz.1        nagios-plugins-2.2.1.tar.gz
email-2.5.1.tar.gz   nagios-plugins-2.1.4         nrpe-3.2.1.tar.gz
nagios-4.4.1         nagios-plugins-2.1.4.tar.gz  pnp4nagios-0.6.26
nagios-4.4.1.tar.gz  nagios-plugins-2.2.1         pnp4nagios-0.6.26.tar.gz
root@ubuntu:/home/nagios#
```

APÊNDICE E – Instalação dependencias

```
root@ubuntu:/home/nagios# apt-get install apache2 build-essential php libgd-dev
unzip postfix s-nail unzip libapache2-mod-php7.0 traceroute
Lendo listas de pacotes... Pronto
Construindo Ã¡rvore de dependÃªncias
Lendo informaÃ§Ã£o de estado... Pronto
```

APÊNDICE F – Criar Usuário

```
root@ubuntu:/home/nagios# useradd  nagios
useradd: user 'nagios' already exists
root@ubuntu:/home/nagios# groupadd nagcmd
groupadd: group 'nagcmd' already exists
root@ubuntu:/home/nagios# passwd nagios
Digite a nova senha UNIX:
Redigite a nova senha UNIX:
passwd: password updated successfully
root@ubuntu:/home/nagios# usermod -a -G nagcmd nagios
root@ubuntu:/home/nagios# usermod -a -G nagios  www-data
root@ubuntu:/home/nagios#
```

APÊNDICE G – Compilar Arquivo

```
root@ubuntu:/home/nagios# cd nagios-4.4.1/
root@ubuntu:/home/nagios/nagios-4.4.1# ./configure --prefix=/usr/local/nagios --
with-httpd-conf=/etc/apache2/sites-enabled/ --with-command-group=nagcmd --with-m
ail=/usr/bin/mail

root@ubuntu:/home/nagios/nagios-4.4.1# make all

root@ubuntu:/home/nagios/nagios-4.4.1# make install
root@ubuntu:/home/nagios/nagios-4.4.1# make install-init
root@ubuntu:/home/nagios/nagios-4.4.1# make install-config
root@ubuntu:/home/nagios/nagios-4.4.1# make install-commandmode
root@ubuntu:/home/nagios/nagios-4.4.1# make install-webconf
root@ubuntu:/home/nagios/nagios-4.4.1# cp -R contrib/eventhandlers/ /usr/local/n
agios/libexec/
```

```
root@ubuntu:/home/nagios/nagios-4.4.1# chown -R nagios:nagios /usr/local/nagios/
libexec/eventhandlers
```

APÊNDICE H– Comando de Teste

```
root@ubuntu:/home/nagios/nagios-4.4.1# /usr/local/nagios/bin/nagios -v /usr/loca
l/nagios/etc/nagios.cfg
```

APÊNDICE I– Instalação Plugins

```
root@ubuntu:/home/nagios# cd nagios-plugins-2.1.4/
root@ubuntu:/home/nagios/nagios-plugins-2.1.4#
```

```
root@ubuntu:/home/nagios# cd nagios-plugins-2.1.4/
root@ubuntu:/home/nagios/nagios-plugins-2.1.4#
```

```
root@ubuntu:/home/nagios/nagios-plugins-2.1.4# make && make install
```

APÊNDICE J– Acessar Interface do Nagios pela Web

```
root@ubuntu:/home/nagios/nagios-plugins-2.1.4# htpasswd -c /usr/local/nagios/etc
/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
root@ubuntu:/home/nagios/nagios-plugins-2.1.4#
```

APÊNDICE L– Módulos CGI – REWRITEE

```
root@ubuntu:/home/nagios/nagios-plugins-2.1.4# a2enmod rewrite cgi
```

```
root@ubuntu:/home/nagios/nagios-plugins-2.1.4# /etc/init.d/apache2 restart
```

```
root@ubuntu:/home/nagios/nagios-plugins-2.1.4# cd /etc/init.d/
```

```
root@ubuntu:/home/nagios/nagios-plugins-2.1.4# rm -rf nagios
```

```
root@ubuntu:/home/nagios/nagios-plugins-2.1.4# cp -p skeleton nagios
```

```
root@ubuntu:/etc/init.d# nano nagios
```

```
DESC="Nagios"
NAME=nagios
DAEMON=/usr/local/nagios/bin/$NAME
DAEMON_ARGS="-d /usr/local/nagios/etc/nagios.cfg"
PIDFILE=/usr/local/nagios/var/$NAME.lock
```

```
root@ubuntu:/etc/init.d# chmod 755 nagios
```

```
root@ubuntu:/etc/init.d# update-rc.d nagios defaults
root@ubuntu:/etc/init.d# /etc/init.d/nagios start
```

APÊNDICE M– Acesso ao Nagios Tela Inicial