

Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

André Luiz Rodrigues da Silva Vieira

**ADMINISTRAÇÃO E GERÊNCIA DE REDES DE
COMPUTADORES**

Rio de Janeiro

2010

André Luiz Rodrigues da Silva Vieira

ADMINISTRAÇÃO E GERÊNCIA DE REDES DE COMPUTADORES

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Rio de Janeiro

2010

André Luiz Rodrigues da Silva Vieira

ADMINISTRAÇÃO E GERÊNCIA DE REDES DE COMPUTADORES

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em Março de 2010.



Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

RESUMO

VIEIRA, André Luiz Rodrigues da Silva. **ADMINISTRAÇÃO E GERÊNCIA DE REDES DE COMPUTADORES**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

Com a crescente complexidade das redes de computadores, a utilização de sistemas de gerenciamento de redes torna-se cada vez mais indispensável. Esta monografia apresenta estudos de caso onde é mostrada a importância da utilização de ferramentas de gerenciamento de redes, como o Nagios, o Cacti e o BigBrother, a fim de evitar o consumo excessivo de tempo e recursos para esta tarefa, elevando significativamente o padrão de qualidade do trabalho do administrador, permitindo-o ter uma visão precisa e centralizada de todos os elementos importantes da rede.

ABSTRACT

VIEIRA, André Luiz Rodrigues da Silva. **ADMINISTRAÇÃO E GERÊNCIA DE REDES DE COMPUTADORES**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

With the computers networks growing in complexity, the network monitoring tools usage becomes more and more necessary.

This monograph presents case studies where the importance of using network monitoring tools, like Nagios, Cacti and BigBrother, is shown in order to avoid excessive time and resources demand on managing networks. Enhancing substantially the administrator work quality standard, allowing him having a precise and centralized vision of all important network elements.

LISTA DE FIGURAS

	Página
Figura 1 – Hierarquia ISO	15
Figura 2 – Ramificação do nó MIB II	17
Figura 3 – Gerente e Agentes	20
Figura 4 - Relacionamento de um gerente com o objeto gerenciado	21
Figura 5 - Relacionamento entre gerente e agente baseado no modelo TCP/IP	21
Figura 6 - As operações entre gerente e agente	22
Figura 7 - Mensagem SNMP com seus campos e componentes	23
Figura 8 – Mensagem SNMP v3	26
Figura 9 – Nagios apresentando alertas em equipamentos de clientes da Huthil	29
Figura 10 – Nagios apresentando os equipamentos monitorados dos clientes da Huthil	29
Figura 11 – Nagios apresentando um esquema dos equipamentos dos clientes monitorados pela VPN	30
Figura 12 – Nagios apresentando alertas em serviços de rede nos clientes da Huthil	31
Figura 13 – Interface Web mostrando os equipamentos dos clientes da Huthil	32
Figura 14 – Gráfico de tráfego de Internet de um cliente	33
Figura 15 – Gráfico de espaço em disco de um equipamento de um cliente	33
Figura 16 – Gráfico de utilização de CPU por um equipamento de um cliente	34
Figura 17 – Relatório Mensal – pag. 1	35
Figura 18 – Relatório Mensal – pag. 2	36
Figura 19 – Relatório Mensal – pag. 3	37
Figura 20 – Utilização de CPU de equipamento	40
Figura 21 – Utilização de disco de um equipamento	41
Figura 22 – Utilização de disco de um equipamento	42

LISTA DE TABELAS

Tabela 1 – Ramificação do nó MIB II	Página 17
Tabela 2 – RFCs do SNMP v2	26

SUMÁRIO

	Página
1 INTRODUÇÃO	9
2 REFERENCIAL TEÓRICO	10
2.1 INTRODUÇÃO	10
2.2 FCAPS	10
2.2.1 Gerenciamento de Falhas	11
2.2.2 Gerenciamento de Configuração	11
2.2.3 Gerenciamento de Contabilização	12
2.2.4 Gerenciamento de Desempenho	12
2.2.5 Gerenciamento de Segurança	13
2.3 MIB – MANAGEMENT INFORMATION BASE	13
2.3.1 Definição	13
2.3.2 Construção	14
2.3.3 Estrutura	15
2.3.4 MIB II	16
2.4 SNMP – SIMPLE NETWORK MANAGEMENT PROTOCOL	19
2.4.1 Definição	19
2.4.2 O Agente	20
2.4.3 O Gerente	20
2.4.4 Operações do Protocolo SNMP	21
2.4.5 Mensagens no Protocolo SNMP	23
2.4.6 Limitações do SNMP v1	24
2.4.7 SNMP v2	24
2.4.7.1 Transmissão de Dados Complexos	25
2.4.7.2 Gerenciamento Descentralizado de Redes	25
2.4.8 SNMP v3	26
3 ESTUDO DE CASO	27
3.1 HUTHIL TECNOLOGIA	27
3.1.1 Monitoramento pela Ferramenta Nagios.	27
3.1.2 Monitoramento pela Ferramenta Cacti.	31
3.1.3 Exemplo de relatório sobre monitoramento mensal de cliente	34
3.2 GOLDEN CROSS	38
3.2.1 Monitoramento pela Ferramenta Big Brother	39
3.2.2 Exemplo de Formulário de Requisição de Mudanças	43
3.2.3 Exemplo de Relatório de Incidente	45
4 CONCLUSÃO	47
5 REFERÊNCIAS BIBLIOGRÁFICAS	48

1 INTRODUÇÃO

Devido às vantagens e facilidades que as redes de computadores oferecem, a adoção e crescimento das mesmas são estimulados tornando seus recursos e aplicações cada vez mais indispensáveis para as organizações.

Em um ambiente com poucas máquinas conectadas em rede, uma única pessoa é capaz de gerenciá-las. Mas, na proporção que as redes se tornam maiores (extensão), complexas (tecnologia), heterogêneas (plataformas de hardware e software distintas) e distribuídas (entre várias salas, prédios e até localidades distintas), tornam o gerenciamento e manutenção onerosos consumindo tempo e recursos, podendo levá-las a um estado de inoperância ou a níveis inaceitáveis de desempenho.

A utilização de ferramentas específicas para gerência de redes é um recurso indispensável na vida de um administrador de redes. E este trabalho tem como finalidade apresentar a importância da utilização de tais ferramentas na gerência de redes corporativas.

Nesta monografia, serão analisadas as seguintes ferramentas: **Nagios**, **Cacti** e **Big Brother**.

2 REFERENCIAL TEÓRICO

2.1 INTRODUÇÃO

Em 1988, a IETF (Internet Engineering Task Force) propôs o protocolo SNMP (Simple Network Management Protocol) [1], que acabou por se tornar o padrão de fato para o gerenciamento de redes IP. O SNMP foi concebido para fornecer fácil implantação e baixo custo para ser implantado nos diversos dispositivos de gerenciamento de redes como roteadores, switches, servidores, estações de trabalho e outros dispositivos de rede. A especificação do SNMP define:

- Um protocolo para troca de informações entre um ou mais gerenciadores de sistema (gerentes) e vários elementos gerenciáveis no sistema (agentes);
- Um mecanismo para formatar e armazenar informações de gerenciamento (MIB);
- Um número de objetos ou variáveis para manipular as informações.

Em 1989, a ISO (International Standards Organization), com o propósito de gerenciar redes, serviços e equipamentos heterogêneos, operando sobre os mais diversos fabricantes e tecnologias que já possuem alguma funcionalidade de gerência, propôs um modelo de referência publicado no OSI Management Framework (Open Systems Interconnection), dividindo as tarefas e processos de gerenciamento em cinco áreas funcionais, ficando conhecido como FCAPS.

2.2 FCAPS

A gerência de uma rede envolve atividades agrupadas em cinco áreas funcionais:

- *Fault* (Gerenciamento de falhas);
- *Configuration* (Gerenciamento de configuração);
- *Accounting* (Gerenciamento de contabilização);
- *Performance* (Gerenciamento de desempenho);
- *Security* (Gerenciamento de segurança).

As atividades de cada área têm por objetivo controlar a rede, otimizar a sua utilização e melhorar o desempenho dos serviços prestados aos usuários.

2.2.1 Gerenciamento de Falhas

O gerenciamento de falhas engloba as funções de detecção, isolamento e correção de operações anormais na rede. As falhas impedem que os sistemas funcionem de modo a cumprir seus objetivos operacionais. As funções de gerenciamento de falhas podem ser divididas em:

- Supervisão de alarmes: gerenciamento de informações sobre as degradações de desempenho que afetam o serviço;
- Teste: o usuário pode solicitar a execução de um teste específico, podendo inclusive estabelecer os parâmetros. Em alguns casos, o tipo e os parâmetros do teste podem ser designados automaticamente;
- Relatório de problemas: utilizado para rastrear e controlar as ações tomadas para liberar alarmes e outros problemas.

Algumas funções do gerenciamento de falhas são:

- Manter os logs dos sistemas;
- Monitorar e agir sobre as notificações de erros;
- Rastrear e identificar falhas;
- Gerar seqüências de testes de diagnóstico;
- Corrigir as falhas encontradas.

2.2.2 Gerenciamento de Configuração

Caracteriza-se pelo conjunto de operações necessárias para a inicialização, término, alteração e armazenamento da configuração dos equipamentos da rede.

Como benefício do gerenciamento de configuração tem-se a fácil alteração na configuração dos equipamentos, o fácil acesso à documentação sobre a configuração dos equipamentos e a manutenção de um inventário atualizado.

Para o gerenciamento de configuração têm-se as seguintes opções básicas:

- Coleta de dados da rede;
- Inicializar e alterar a configuração de equipamentos;
- Manter banco de dados sobre configuração de equipamentos da rede.

Problemas comuns relacionados à configuração:

- Configurações erradas acarretam em falhas;
- Upgrades não documentados.

2.2.3 Gerenciamento de Contabilização

É a área responsável por fazer medições na rede visando estabelecer parâmetros quanto à utilização da rede para, se necessário, determinar cotas, grupos e usuários, procurando uma melhor distribuição dos recursos da rede.

Dentre os muitos recursos que podem ser gerenciados tem-se o espaço em disco, o tempo de conexão, a quantidade de conexões, o tempo de processamento e a utilização da banda.

Para realizar o gerenciamento de contabilização deve-se fazer três operações básicas:

- Coletar dados da rede;
- Analisar os dados coletados;
- Contabilizar por usuários, grupos, departamentos, etc.

Um dos problemas mais comuns relacionados a contabilização é a falta de informações para auxiliar no gerenciamento da rede:

- Espaço em disco;
- Tempo de conexão;
- Quantidade de conexões;
- Consumo de memória e CPU do equipamento;
- Utilização da banda;
- Uso indevido dos recursos de navegação e de email.

2.2.4 Gerenciamento de Desempenho

Define-se pelo conjunto de funções necessárias para o gerente de rede monitorar e analisar as atividades na rede, fazendo os devidos ajustes necessários.

A prevenção de congestionamentos e a necessidade de prever o crescimento da rede são os benefícios oferecidos por este gerenciamento.

Para esta tarefa é necessária a coleta de dados na rede, de forma aleatória, respeitando regras estatísticas que possibilitarão avaliar a situação da rede.

Problemas comuns:

- Tempo de resposta das aplicações muito longo;
- Sistemas que demandam muito processamento;
- Demora na realização dos serviços;
- Enorme demanda de acesso a Web;

- Envio ou recebimento de emails com grandes anexos.

2.2.5 Gerenciamento de Segurança

É o conjunto de funções que o gerente de rede deve executar para identificar e proteger equipamentos e dados da rede de ataques e violações oriundas de pessoas não autorizadas.

Para isto deve-se limitar o acesso aos equipamentos, contas de usuários e base de dados com ferramentas adequadas como firewall, proxy e outros softwares de segurança.

Os principais procedimentos que devem ser executados para o gerenciamento de segurança são:

- Identificar informações e equipamentos que devem ser protegidos;
- Encontrar possíveis pontos vulneráveis de acesso a rede e protegê-los;
- Manter a rede protegida.

Problemas comuns:

- Ataques;
- Vírus;
- Perdas de dados;
- Perda de Servidores ou estações;
- Indisponibilidade de algum serviço;

2.3 MIB – MANAGEMENT INFORMATION BASE

2.3.1 Definição

Antes de definir o que é uma MIB, será mostrado o conceito de objetos gerenciados.

Um objeto gerenciado é a visão abstrata de um recurso real do sistema. Assim, todos os recursos da rede que devem ser gerenciados são modelados, e as estruturas dos dados resultantes são os objetos gerenciados. Os objetos gerenciados podem ter permissões para serem lidos ou alterados, sendo que cada leitura representará o estado real do recurso e, cada alteração também será refletida no próprio recurso.

Dessa forma, a MIB é o conjunto dos objetos gerenciados que procura abranger todas as informações necessárias para a gerência da rede.

O RFC 1066 [2] apresentou a primeira versão da MIB, a MIB I. Este padrão explicou e definiu a base de informação necessária para monitorar e controlar redes baseadas na pilha de protocolos TCP/IP. A evolução aconteceu com o RFC 1213 [3] que propôs uma segunda MIB, a MIB II, para uso baseado na pilha de protocolos TCP/IP.

Basicamente são definidos três tipos de MIBs: MIB II, MIB experimental, MIB privada.

A MIB II, que é considerada uma evolução da MIB I, fornece informações gerais de gerenciamento sobre um determinado equipamento gerenciado. Através das MIB II podemos obter informações como: número de pacotes transmitidos, estado da interface, entre outras.

A MIB experimental é aquela em que seus componentes (objetos) estão em fase de desenvolvimento e teste. Em geral, fornecem características mais específicas sobre a tecnologia dos meios de transmissão e equipamentos empregados.

MIB privada é aquela em que seus componentes fornecem informações específicas dos equipamentos gerenciados, como configuração, colisões e também é possível reinicializar, desabilitar uma ou mais portas de um equipamento.

2.3.2 Construção

As regras de construção das estruturas da MIB são descritas através da SMI - Structure of Management Information [4]. A estrutura de informações de gerência SMI é um conjunto de documentos que definem:

- Forma de identificação e agrupamento das informações;
- Sintaxes permitidas;
- Tipos de dados permitidos.

Os objetos de uma MIB são especificados de acordo com a ASN.1 - Abstract Syntax Notation One. A notação sintática abstrata é uma forma de descrição abstrata dos dados com o objetivo de não se levar em consideração a estrutura e restrições do equipamento no qual está sendo implementada. Para cada objeto são definidos: nome, identificador, sintaxe, definição e acesso. As instâncias do objeto são chamadas de variáveis.

O *Object Name* é o nome do objeto, composto por uma string de texto curto.

O *Object Identifier* é o identificador do objeto, formado por números que são separados por pontos.

A *Syntax* é a sintaxe do objeto que descreve o formato, ou o valor, da informação. Ela pode ser:

- uma sintaxe do tipo simples que pode ser um inteiro, uma string de octetos, um *Object Identifier* ou nulo;
- pode ser também uma sintaxe de aplicação podendo ser um endereço de rede, um contador, uma medida, um intervalo de tempo ou incompreensível.

A *Definition* é uma descrição textual do objeto.

O *Access* é o tipo de controle que se pode ter sobre o objeto, podendo ser: somente leitura, leitura e escrita ou não acessível.

2.3.3 Estrutura

A árvore hierárquica na figura 1 foi definida pela ISO representa a estrutura lógica da MIB, mostra o identificador e o nome de cada objeto.

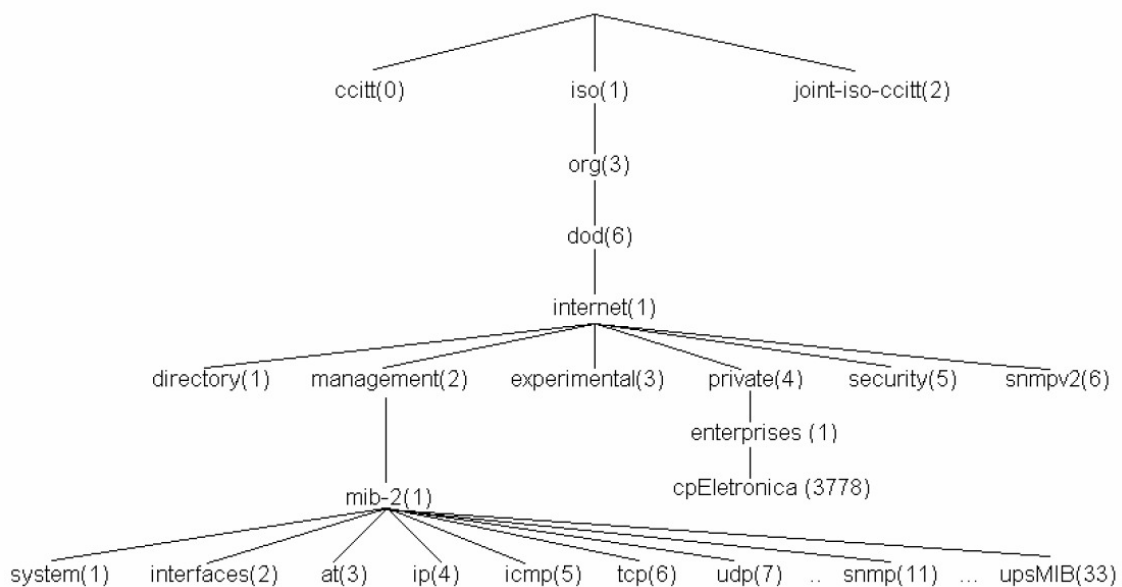


Figura 1 – Hierarquia ISO

O nó raiz da árvore não possui rótulo mas possui pelo menos três subníveis, sendo eles: o nó 0 que é administrado pela Consultative Committee for International Telegraph and Telephone - CCITT; o nó 1 que é administrado pela International

Organization for Standardization – *ISO*; e o nó 2 que é administrado em conjunto pela CCITT e pela ISO. Sob o nó *ISO* fica o nó que pode ser utilizado por outras instituições: o *org* (3), abaixo dele fica o *dod* (6) que pertence ao departamento de defesa dos EUA. O departamento de defesa dos EUA alocou um sub-nó para a comunidade internet, que é administrado pela International Activities Board - IAB e abaixo deste nó temos, entre outros, os nós: *management*, *experimental*, *private*.

Sob o nó *management* ficam as informações de gerenciamento, é sob este nó que está o nó da MIB II.

Sob o nó *experimental* estão as MIBs experimentais.

Sob o nó *private* fica o nó *enterprises* e sob este nó ficam os nós das indústrias de equipamentos.

Como exemplo de um objeto citaremos o *ipInReceives* do grupo IP:

ipInReceives Object Type

Object Identifier: 1.3.6.1.2.1.4.3

Access: read-only

Syntax: Counter32

Description: Número total de datagramas que chegam nas interfaces, incluindo aqueles com erro.

2.3.4 MIB II

Abaixo da subárvore MIB II estão os objetos usados para obter informações específicas dos dispositivos da rede. Esses objetos estão divididos em 10 grupos, que estão presentes na tabela abaixo.

Tabela 1 – Ramificação do nó MIB II

Grupo	Informação
system (1)	informações básicas do sistema
interfaces (2)	interfaces de rede
at (3)	tradução de endereços
ip (4)	protocolo ip
icmp (5)	protocolo icmp
tcp (6)	protocolo tcp
udp (7)	protocolo udp
egp (8)	protocolo egp
transmission (10)	meios de transmissão
snmp (11)	protocolo snmp

A planificação do nó da MIB II é vista na figura 2.

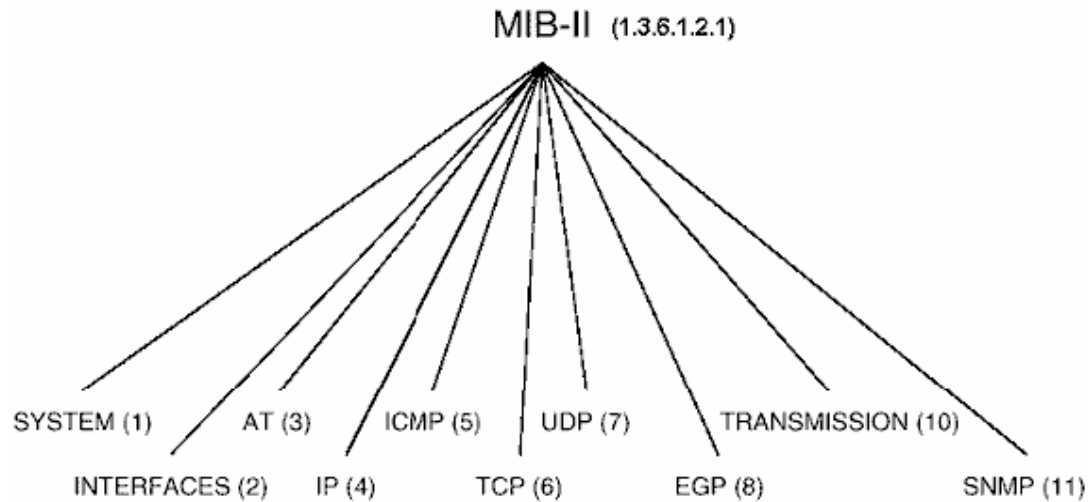


Figura 2 – Ramificação do nó MIB II

Seguem abaixo, alguns exemplos de objetos pertencentes aos grupos da MIB II:

Grupo System (1.3.6.1.2.1.1)

- *sysDescr* (1.3.6.1.2.1.1.1): Descrição textual da unidade. Pode incluir o nome e a versão do hardware, sistema operacional e o programa de rede.
- *sysUpTime* (1.3.6.1.2.1.1.3): Tempo decorrido (em centésimos de segundos) desde a última reinicialização do gerenciamento do sistema na rede.
- *sysContact* (1.3.6.1.2.1.1.4): Texto de identificação do gerente da máquina gerenciada e como contatá-lo.

Grupo Interfaces (1.3.6.1.2.1.2)

- *ifNumber* (1.3.6.1.2.1.2.1): Número de interfaces de rede (não importando seu atual estado) presentes neste sistema.
- *ifOperStatus* (1.3.6.1.2.1.2.2.1.8): Estado atual da interface.
- *ifInOctets* (1.3.6.1.2.1.2.2.1.10): Número total de octetos recebidos pela interface.

Grupo IP (1.3.6.1.2.1.4)

- *ipForwarding* (1.3.6.1.2.1.4.1): Indica se esta entidade é um gateway.

- *ipInReceives* (1.3.6.1.2.1.4.3): Número total de datagramas recebidos pelas interfaces, incluindo os recebidos com erro.
- *ipInHdrErrors* (1.3.6.1.2.1.4.4): Número de datagramas que foram recebidos e descartados devido a erros no cabeçalho IP.

Grupo ICMP (1.3.6.1.2.1.5)

- *icmpInMsgs* (1.3.6.1.2.1.5.1): Número total de mensagens ICMP recebidas por esta entidade. Incluindo aquelas com erros.
- *icmpOutMsgs* (1.3.6.1.2.1.5.14): Número total de mensagens ICMP enviadas por esta entidade. Incluindo aquelas com erros.

Grupo TCP (1.3.6.1.2.1.6)

- *tcpMaxConn* (1.3.6.2.1.6.4): Número máximo de conexões TCP que esta entidade pode suportar.
- *tcpCurrentEstab* (1.3.6.2.1.6.9): Número de conexões TCP que estão como estabelecidas ou a espera de fechamento.
- *tcpRetransSegs* (1.3.6.2.1.6.12): Número total de segmentos retransmitidos.

Grupo UDP (1.3.6.1.2.1.7)

- *udpInDatagrams* (1.3.6.1.2.1.7.1): Número total de datagramas UDP entregues aos usuários UDP.
- *udpNoPorts* (1.3.6.1.2.1.7.2): Número total de datagramas UDP recebidos para os quais não existia aplicação na referida porta.
- *udpLocalPort* (1.3.6.1.2.1.7.5.1.2): Número da porta do usuário UDP local.

Grupo SNMP (1.3.6.1.2.1.11)

- *snmpInPkts* (1.3.6.1.2.1.11.1): Número total de mensagens recebidas pela entidade SNMP.
- *snmpOutPkts* (1.3.6.1.2.1.11.2): Número total de mensagens enviadas pela entidade SNMP.
- *snmpInTotalReqVars* (1.3.6.1.2.1.11.13): Número total de objetos da MIB que foram resgatados pela entidade SNMP.

2.4 SNMP – SIMPLE NETWORK MANAGEMENT PROTOCOL

2.4.1 Definição

Este protocolo tem como premissa a flexibilidade e a facilidade de implementação, também em relação aos produtos futuros. Sua especificação está contida no RFC 1157 [1].

O SNMP é um protocolo de gerência definido a nível de aplicação, é utilizado para obter informações de servidores SNMP - agentes espalhados em uma rede baseada na pilha de protocolos TCP/IP. Os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte UDP - User Datagram Protocol - para enviar e receber suas mensagens através da rede. Dentre as variáveis que podem ser requisitadas utilizaremos aquelas definidas nas MIBs, podendo fazer parte da MIB II, da experimental ou da privada.

O gerenciamento da rede através do SNMP permite o acompanhamento simples e fácil do estado, em tempo real, da rede, podendo ser utilizado para gerenciar diferentes tipos de sistemas.

Este gerenciamento é conhecido como modelo de gerenciamento SNMP, ou simplesmente, gerenciamento SNMP. Portanto, o SNMP é o nome do protocolo no qual as informações são trocadas entre a MIB e a aplicação de gerência como também é o nome deste modelo de gerência.

Os comandos são limitados e baseados no mecanismo de busca/alteração. No mecanismo de busca/alteração estão disponíveis as operações de alteração de um valor de um objeto, de obtenção dos valores de um objeto e suas variações.

A utilização de um número limitado de operações, baseadas em um mecanismo de busca/alteração, torna o protocolo de fácil implementação, simples, estável e flexível. Como consequência reduz o tráfego de mensagens de gerenciamento através da rede e permite a introdução de novas características.

O funcionamento do SNMP é baseado em dois dispositivos: o agente e o gerente. Cada máquina gerenciada é vista como um conjunto de variáveis que representam informações referentes ao seu estado atual, que ficam disponíveis ao gerente através de consulta e podem ser alteradas por ele. Cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB.

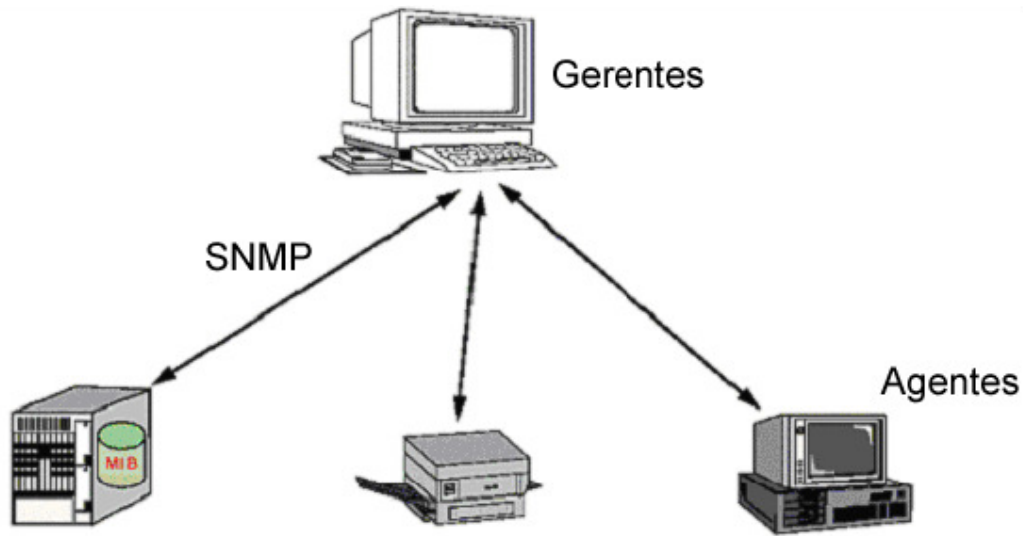


Figura 3 – Gerente e Agentes

2.4.2 O Agente

É um processo executado na máquina gerenciada, responsável pela manutenção das informações de gerência da máquina. As funções principais de um agente são:

- Atender as requisições enviadas pelo gerente;
- Enviar automaticamente informações de gerenciamento ao gerente, quando previamente programado;

O agente utiliza as chamadas de sistema para realizar o monitoramento das informações da máquina e utiliza as RPC (Remote Procedure Call) para o controle das informações da máquina.

2.4.3 O Gerente

É um programa executado em uma estação servidora que permite a obtenção e o envio de informações de gerenciamento junto aos dispositivos gerenciados mediante a comunicação com um ou mais agentes.

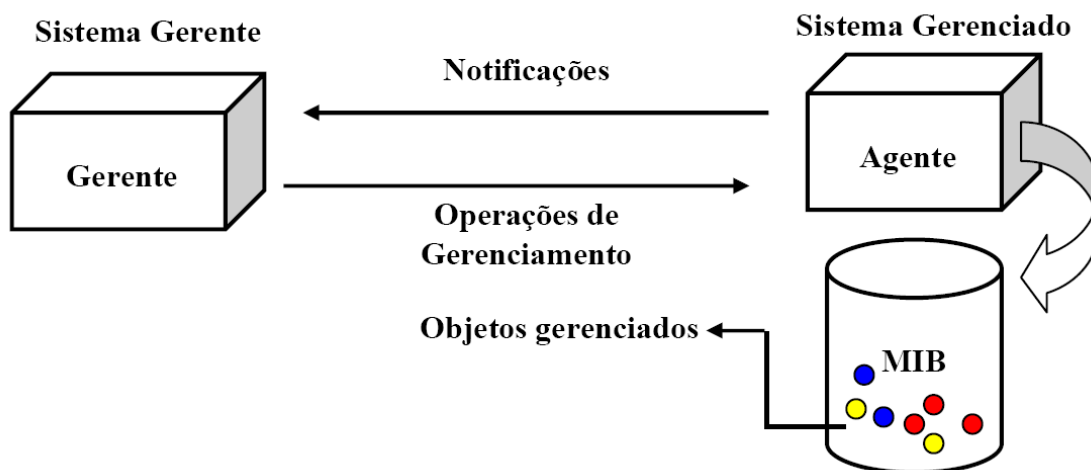


Figura 4 - Relacionamento de um gerente com o objeto gerenciado

O gerente fica responsável pelo monitoramento, relatórios e decisões na ocorrência de problemas, enquanto que o agente fica responsável pelas funções de envio e alteração das informações e também pela notificação da ocorrência de eventos específicos ao gerente.

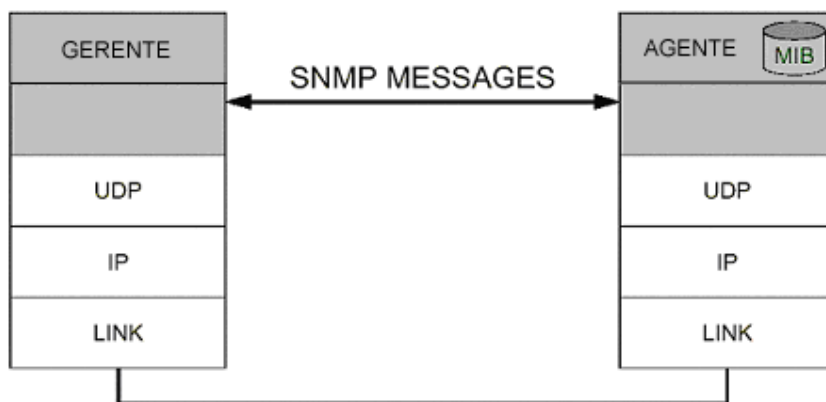


Figura 5 - Relacionamento entre gerente e agente baseado no modelo TCP/IP

2.4.4 Operações do Protocolo SNMP

Existem duas operações básicas (SET e GET) e suas derivações (GET-NEXT, TRAP).

- A operação SET é utilizada para alterar o valor da variável; o gerente solicita que o agente faça uma alteração no valor da variável;
- A operação GET é utilizada para ler o valor da variável; o gerente solicita que o agente obtenha o valor da variável;

- A operação de GET-NEXT é utilizada para ler o valor da próxima variável; o gerente fornece o nome de uma variável e o cliente obtém o valor e o nome da próxima variável; também é utilizado para obter valores e nomes de variáveis de uma tabela de tamanho desconhecido;
- A operação TRAP é utilizada para comunicar um evento; o agente comunica ao gerente o acontecimento de um evento previamente determinado. São sete tipos básicos de trap determinados:
 - *coldStart*: a entidade que a envia foi reinicializada, indicando que a configuração do agente ou a implementação pode ter sido alterada;
 - *warmStart*: a entidade que a envia foi reinicializada, porém a configuração do agente e a implementação não foram alteradas;
 - *linkDown*: o enlace de comunicação foi interrompido;
 - *linkUp*: o enlace de comunicação foi estabelecido;
 - *authenticationFailure*: o agente recebeu uma mensagem SNMP do gerente que não foi autenticada;
 - *egpNeighborLoss*: um par EGP (Exterior Gateway Protocol) parou;
 - *enterpriseSpecific*: indica a ocorrência de uma operação TRAP não básica.

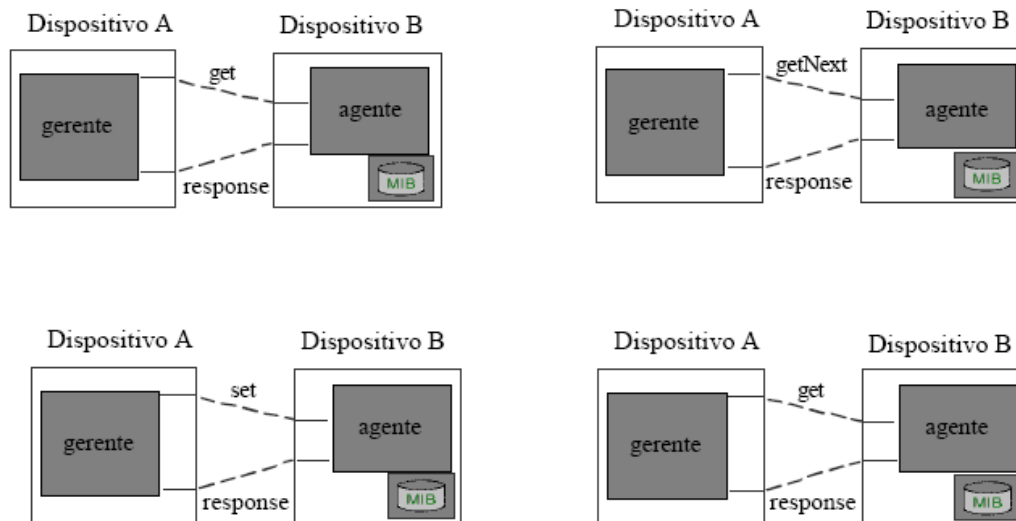


Figura 6 - As operações entre gerente e agente

2.4.5 Mensagens no Protocolo SNMP

Uma mensagem SNMP deve definir o agente do qual vai se obter ou alterar os atributos dos objetos, e que será o responsável pela conversão das operações requisitadas em operações sobre a MIB. Após verificar os campos de uma mensagem o agente deve utilizar as estruturas internas disponíveis para interpretar a mensagem e enviar a resposta da operação ao gerente que a solicitou.

As mensagens no protocolo SNMP não possuem campos fixos e por isso são construídas de trás para frente. A mensagem possui três partes principais: *version*, *community*, *SNMP PDU*.

- A *version* contém a versão do SNMP. Tanto o gerente como o agente devem utilizar a mesma versão. Mensagens contendo versões diferentes são descartadas;
- A *community* que identifica a comunidade. É utilizada para permitir acesso do gerente as MIBs, como uma senha de acesso;
- A *SNMP PDU* é a parte dos dados. Possui PDU (Protocol Data Units) que são constituídas por um pedido ou por uma resposta a um pedido.

campos variáveis:

NOME 1	VALOR 1	NOME 2	VALOR 2	NOME n	VALOR n
--------	---------	--------	---------	-----	-----	--------	---------

PDU SNMP:

Tipo de PDU	ID da Requisição	Status do Erro	Índice do Erro	Campos Variáveis
-------------	------------------	----------------	----------------	------------------

Mensagem SNMP:

VERSION	COMMUNITY	SNMP PDU
---------	-----------	----------

Figura 7 - Mensagem SNMP com seus campos e componentes

Existem cinco tipos de PDUs: *GetRequest*, *GetNextRequest*, *GetResponse*, *SetRequest* e *Trap*. Com dois formatos distintos.

O formato das PDUs *GetRequest*, *GetNextRequest*, *GetResponse* e *SetRequest*:

Tipo de PDU	ID da Requisição	Status do Erro	Índice do Erro	Objeto 1, Valor 1	Objeto 2, Valor 2	...
-------------	------------------	----------------	----------------	-------------------	-------------------	-----

O formato da PDU *Trap*:

Tipo de PDU	Enterprise	Endereço do Agente	Trap Genérica	Trap Específica	Time Stamp	Obj 1, Val 1	Obj 2, Val 2	...
-------------	------------	--------------------	---------------	-----------------	------------	--------------	--------------	-----

2.4.6 Limitações do SNMP v1

O SNMP v1 não é apropriado para o gerenciamento de redes muito grandes devido à limitação de performance de *pooling* e não suporta comunicação manager-to-manager, que garantiria um gerenciamento descentralizado.

Como provê somente autenticação trivial, essa versão é deficiente nas questões de segurança de acesso às informações gerenciadas. O modelo SNMP MIB é limitado e não suporta aplicações que questionam o gerenciamento baseadas em valores ou tipos de objetos

2.4.7 SNMP v2

O SNMP v1 proliferou-se rapidamente, pois surgiu como uma ferramenta simples para gerenciamento de redes. A primeira versão ofereceu funções de fácil implementação, fácil uso e sua simplicidade não prejudica o desempenho da rede. Após o início dessa utilização pelos administradores de redes, notaram-se algumas falhas e a necessidade de novas funcionalidades. Entre elas a necessidade da transferência de dados complexos, a comunicação entre gerentes e questões de segurança. As duas primeiras necessidades foram implementadas na SNMPv2, como mostradas na Tabela 2 [5][6][7][8][9][10][11][12].

Tabela 2 – RFCs do SNMP v2

RFC		Data
1901	Introduction to Community-based SNMPv2.	Janeiro 1996
1902	Structure of Management Information for Version 2 of Simple Network Management Protocol (SNMPv2)	Janeiro 1996
1903	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)	Janeiro 1996
1904	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)	Janeiro 1996
1905	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)	Janeiro 1996
1906	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)	Janeiro 1996
1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)	Janeiro 1996
1908	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework.	Janeiro 1996

2.4.7.1 Transmissão de Dados Complexos

A implementação da transmissão de dados complexos no SNMPv2 obteve um impacto positivo no quesito de consumo de recursos da rede, pois na versão anterior, caso fosse necessário a transferência de uma tabela de dados, a transferência se daria mensagem a mensagem até que todos os elementos fossem transferidos, o que na implementação do SNMPv2 não é mais necessário: o comando *get-bulk* foi implementado para suprir essa necessidade. Um exemplo da utilização desse novo comando seria um gerente solicitando a um agente alocado em um roteador a sua tabela de roteamento.

2.4.7.2 Gerenciamento Descentralizado de Redes

Quando uma rede cresce enormemente, tanto em dispositivos conectados a ela e quanto ao tráfego que por ela passa, o gerenciamento centralizado já não é o mais ideal, pois só um gerente teria que lidar com todos os dispositivos. O tráfego por ele gerado seria alto, como também este gerente precisaria realizar muitas

tarefas. No SNMP v2, com a adição do suporte a comunicação manager-to-manager, ou seja, comunicação entre estações de gerenciamento, uma abordagem de gerenciamento descentralizado poderia ser adotado.

2.4.8 SNMP v3

O SNMP v2 supriu várias deficiências da sua versão antecessora, mas não uma muito importante: segurança. As questões de segurança foram implementadas somente no SNMP v3. Esta versão consiste em três módulos: processamento e controle das mensagens, o processamento local e segurança.

O primeiro módulo, processamento e controle das mensagens, é responsável pelas funções de criação e análise gramatical das mensagens. O segundo módulo, processamento local, é responsável pelo controle de acesso às variáveis da mensagem, faz o processamento desses dados e é responsável pelo processamento das traps. Por último, o módulo de segurança tem a função de criptografia e autenticação das mensagens.

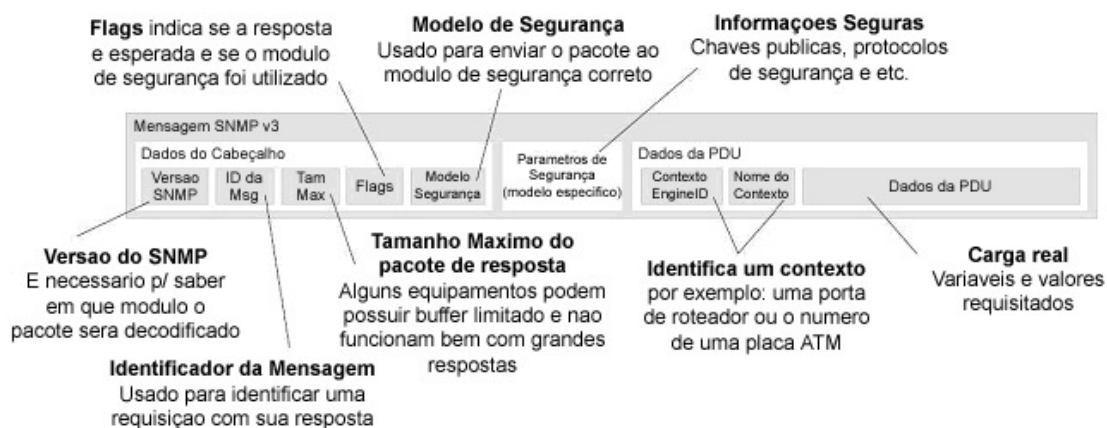


Figura 8 – Mensagem SNMP v3

As características de segurança implementadas pelo SNMP v3 são: autenticação, criptografia e controle de acesso. Para esta nova versão, um formato de mensagem diferente foi adotado como visto na Figura 8.

3 ESTUDO DE CASO

O estudo de caso apresenta a utilização das ferramentas **Nagios**, **Cacti** e **Big Brother** pela equipe de Administração de Redes de duas empresas: a Huthil Tecnologia Ltda e a Golden Cross Assistência Internacional de Saúde Ltda.

3.1 HUTHIL TECNOLOGIA

É uma empresa de consultoria em TI que atua no mercado há mais de 10 anos e tem como principal atividade o suporte às redes dos seus clientes. Para que a atividade de gerenciamento das redes de seus clientes seja exercida atendendo o SLA (Service License Agreement) contratado, todos os clientes estão conectados ao escritório da Huthil através de VPN, onde está montado um NOC (Network Operation Center), utilizando os softwares Nagios e Cacti para o monitoramento dos ambientes destes clientes.

Uma vez detectado um alerta e dependendo da falha apresentada, a equipe técnica pode resolver o problema remotamente se valendo da VPN ou um analista é enviado imediatamente ao local para a intervenção presencial.

No caso de serviços de rede não críticos, isto é, serviços que mesmo parados afetam muito pouco o andamento dos trabalhos da atividade fim do cliente, esses serviços normalmente possuem um SLA de atendimento máximo em até 4 horas. Enquanto que os serviços de rede de missão crítica, isto é, serviços que se parados afetam fortemente a atividade fim do cliente, podendo até paralisar os trabalhos do cliente, possuem SLA de atendimento máximo em até 1 hora.

Ao final de todo mês a gerencia da Huthil Tecnologia envia um relatório a seus clientes informando as estatísticas de suas respectivas redes em conformidade ao contrato de serviço firmado entre eles.

3.1.1 Monitoramento pela Ferramenta Nagios.

O Nagios [13] é uma aplicação desenvolvida para monitoramento de rede. Ela pode monitorar equipamentos e serviços, enviando notificações de eventos. Algumas de suas principais características são:

- Monitoramento de serviços de rede (SMTP, HTTP, DNS, etc.);
- Monitoramento dos recursos dos equipamentos (carga de CPU, espaço em disco, utilização de memória, etc.);
- Notificações quando ocorrem problemas em equipamentos e serviços;

- Definição de eventos que serão disparados durante sua ocorrência em equipamentos e serviços;
- Geração de logs;
- Interface Web.

É importante salientar que além da área de contabilização, o Nagios atua no gerenciamento de falhas, verificando periodicamente o estado dos recursos monitorados e enviando alertas caso alguma falha ocorra.

O Nagios é também capaz de notificar o administrador caso os valores de utilização de um determinado serviço extrapolem os limites máximos previamente definidos na sua configuração.

Na interface Web do Nagios é possível verificar todas as informações sobre os equipamentos e serviços monitorados, além da configuração geral do sistema. As telas mais relevantes são: *Service Detail*, *Host Detail*, *Status Map* e *Event Log*.

Na tela *Service Detail* são mostrados os serviços monitorados de cada equipamento (figura 9), seu estado que pode ser *OK*, *ALERT* ou *CRITICAL*, a data e hora da última checagem, a duração deste estado e as tentativas de verificação deste estado.

O estado *OK* indica que o serviço monitorado está em ativo e em conformidade com os valores de utilização configurados para seu monitoramento. O estado *ALERT* indica que houve uma falha no serviço monitorado ou foi encontrada uma não-conformidade nos valores de utilização. O estado *CRITICAL* indica que o serviço não está mais respondendo ao monitoramento ou foi encontrada uma não-conformidade grave nos valores de utilização.

Na tela *Host Detail* são mostrados os equipamentos monitorados (figura 10), seu estado que pode ser *UP* ou *DOWN*, a data e hora da última checagem, a duração deste estado e informações adicionais.

O estado *UP* indica que o equipamento está ativo e respondendo ao monitoramento e o estado *DOWN* indica que o equipamento não está ativo ou não está mais respondendo ao monitoramento.

Na tela *Status Map*, é apresentado um desenho esquemático que mostra a dependência dos equipamentos em relação a outros (figura 11). Por exemplo: se um Switch não estiver mais respondendo ao monitoramento, todos os outros equipamentos conectados a ele e dependentes deste para acessar as outras partes

da rede também não mais responderão ao monitoramento, mesmo que não tenham nenhum tipo de problema.

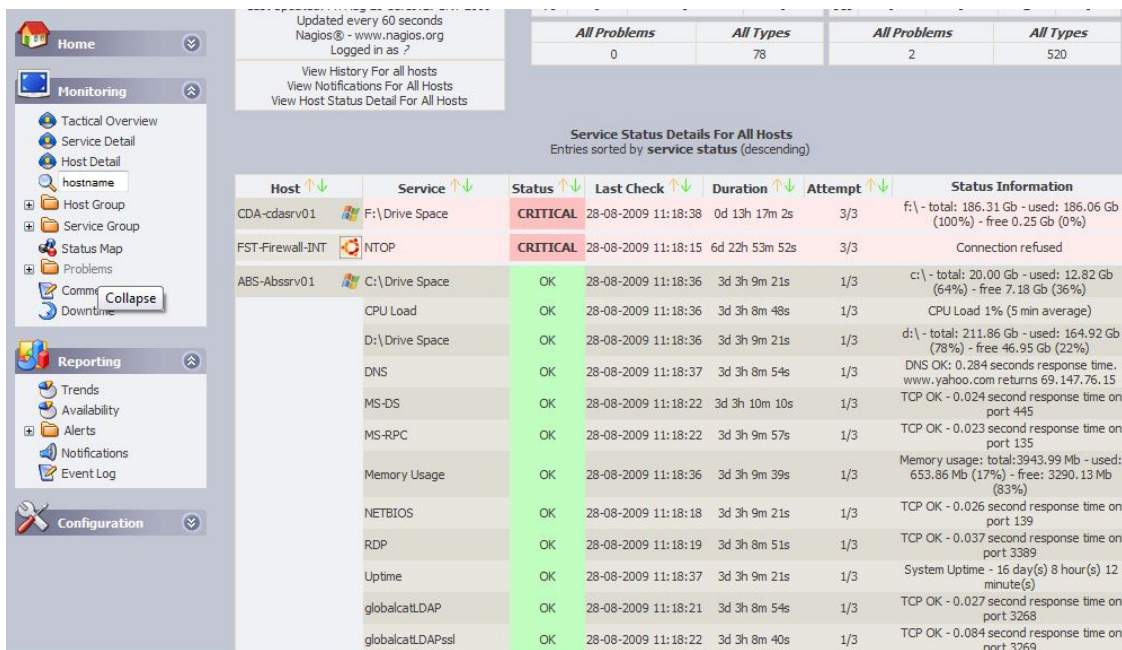


Figura 9 – Nagios apresentando alertas em equipamentos de clientes da Huthil



Figura 10 – Nagios apresentando os equipamentos monitorados dos clientes da Huthil

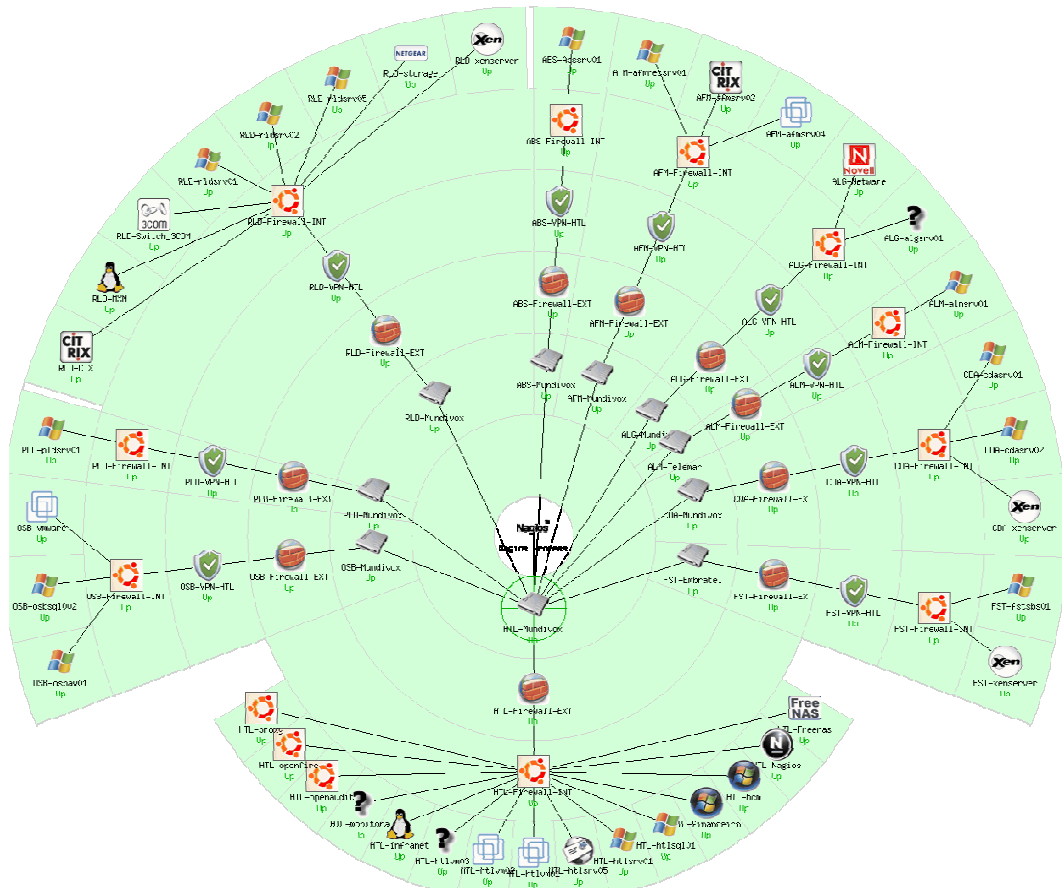


Figura 11 – Nagios apresentando um esquema dos equipamentos dos clientes monitorados pela VPN

Na tela *Event Log*, é possível acompanhar todos os alertas e mudanças de estado que foram detectados pelo Nagios (figura 12). É por meio desta tela que um administrador de rede pode ficar sabendo se um equipamento ou serviço apresentou algum alerta durante um final de semana ou outro período em que não estava utilizando o sistema.



Figura 12 – Nagios apresentando alertas em serviços de rede nos clientes da Huthil

3.1.2 Monitoramento pela Ferramenta Cacti.

O Cacti [14], assim como o Nagios, é uma ferramenta de monitoramento de rede, porém seu enfoque principal está no gerenciamento de contabilização. Exemplos de tipos de informação que podem ser monitorados são: largura de banda, quantidade de emails enviados e recebidos, requisições HTTP, utilização de memória e etc. Os gráficos são gerados em função de intervalos de tempo, produzindo um histórico de monitoramento. As informações coletadas são armazenadas numa base de dados e podem ser consultadas através da interface Web do Cacti. Os gráficos criados podem ainda ser organizados em árvore, sendo útil quando há muitos equipamentos monitorados.

Para que o Cacti possa operar é necessário que o SNMP esteja instalado no servidor de monitoramento e também nos equipamentos monitorados. Uma vez que o Cacti trabalha com SNMP, qualquer informação que este puder recuperar é passível de ser reproduzido em gráfico.

Diferentemente do Nagios, o Cacti não envia alertas em caso de paradas de serviço ou algum outro evento anormal. Contudo ele possui um log que permite que o administrador saiba caso as consultas SNMP não estejam sendo efetuadas com sucesso em algum equipamento.

Dentre as telas do Cacti podemos destacar a tela *Console/Devices* (figura 13), onde são mostrados os equipamentos monitorados e algumas informações sobre eles, dentre as quais as mais importantes são: o *Status* (se o equipamento está ativo ou não), o endereço de rede, seu tempo de resposta ao Cacti, a média desse tempo de resposta e sua disponibilidade, isto é, qual é o percentual de tempo que este equipamento e seus serviços monitorados estão ativos.

The screenshot shows the Cacti web interface for the 'Devices' section. The page title is 'console graphs' and the user is logged in as 'admin'. The main content is a table of devices with the following columns: Description, ID, Graphs, Data Sources, Status, Event Count, Hostname, Current (ms), Average (ms), and Availability. The table lists 39 devices, including various servers, gateways, and backup systems. The status of most devices is 'Up', but 'AFM - Backup' is 'Down'. The interface includes navigation links, search filters, and a 'Choose an action' dropdown at the bottom.

Description**	ID	Graphs	Data Sources	Status	Event Count	Hostname	Current (ms)	Average (ms)	Availability
ABS - DC (File server - DNS - DHCP)	52	5	5	Up	0	10.10.6.51	22.84	54.88	96.85
ABS - Gateway	51	7	13	Up	0	10.10.6.50	22.08	58.87	96.86
AFM - Backup	11	7	7	Down	18200	10.10.3.53	54.1	55.16	60.46
AFM - Citrix	10	10	10	Up	0	10.10.3.52	31.51	55.81	88.33
AFM - DC (File Server, DNS, DHCP e Exchange)	9	8	8	Up	0	10.10.3.51	24.97	65.6	87.79
AFM - Gateway	13	10	18	Up	0	10.10.3.50	78.04	54.58	90.42
ALG - DC (File server - DNS - DHCP)	54	5	5	Up	0	10.10.5.51	20.03	39.99	98.43
ALG - Gateway	23	6	12	Up	0	192.168.0.4	21.25	42.07	91.04
ALM - DC (File server - DNS - DHCP)	35	8	8	Up	0	10.81.17.10	16.38	144.39	84.82
ALM - Gateway	31	8	15	Up	0	10.81.17.7	17.8	68.23	91.34
CDA - Backup, Print Server	27	6	6	Up	0	10.10.11.51	26.06	87.12	86.03
CDA - DC (File Server, DNS, DHCP e Exchange)	28	7	7	Up	0	10.10.9.52	186.43	62.21	85.92
CDA - Gateway	19	6	13	Up	0	10.10.9.50	73.7	63.94	91.23
FTL - Gateway	20	7	14	Up	0	10.10.4.50	56.16	87.67	91.69
FTL - DC (File server - DNS - DHCP)	29	9	9	Up	0	10.10.4.51	324.36	101.77	86.33
HTL - BCM	45	7	7	Up	0	10.10.0.66	11.43	16.01	97.66
HTL - DC (File Server-DNS-DHCP)	6	6	10	Up	0	10.10.0.51	3.22	11.51	91.75
HTL - Financeiro	44	4	4	Up	0	10.10.0.67	7.17	17.36	99.86
HTL - Gateway	8	20	36	Up	0	10.10.0.60	1.51	7.33	99.17
HTL - Servidor CACTI	36	5	11	Up	0	10.10.0.55	1.01	3.14	99.74
HTL - Servidor de Desenvolvimento	17	8	8	Up	0	10.10.0.7	4.4	21.04	93.06
HTL - Servidor de proxy (Huthil)	4	7	14	Up	0	10.10.0.54	51.32	25.91	88.17
HTL - Servidor Exchange(Huthil)	5	9	15	Up	0	10.10.0.50	1.85	24.83	94.17
HTL - Servidor NAGIOS	41	5	11	Up	0	10.10.0.56	1.14	7.27	99.58
HTL - Servidor OPENFIRE	43	5	11	Up	0	10.10.0.62	2.61	4.94	88.85
HTL - Servidor VMWare	18	11	11	Up	0	10.10.0.53	1.47	5.13	88.95
HTL - Servidor VMWARE2	40	6	6	Up	0	10.10.0.63	10.8	3.93	93.69
OSB - DC (File Server-DNS-DHCP)	55	7	7	Up	0	10.10.10.53	26.32	64.09	96.94
OSB - Gateway	37	6	14	Up	0	10.10.10.50	22.44	211.38	94.81
OSB - SQL	39	10	10	Up	0	10.10.10.52	26.32	194.59	94.03

Figura 13 – Interface Web mostrando os equipamentos dos clientes da Huthil

Ao se clicar no nome de cada equipamento, gráficos sobre os serviços monitorados deste equipamento são apresentados. Por exemplo: na figura 14 é apresentado o gráfico do tráfego de internet de um desses clientes. A área verde do gráfico apresenta o tráfego que chega na placa de rede externa deste equipamento,

isto é, o download executado pelos usuários desta rede. A linha em azul apresenta o tráfego que sai desta placa de rede, isto é, o upload executado pelos usuários.

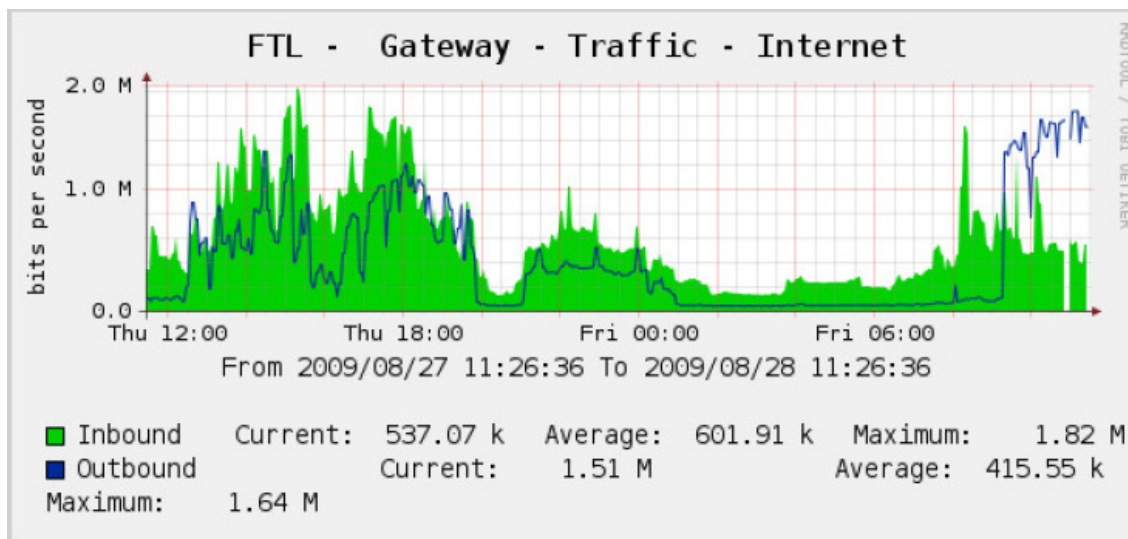


Figura 14 – Gráfico de tráfego de Internet de um cliente

Na figura 15 é apresentado o gráfico do espaço em disco utilizado por este equipamento. A área em azul representa a capacidade disponível do disco e a área em vermelho a capacidade utilizada deste disco.

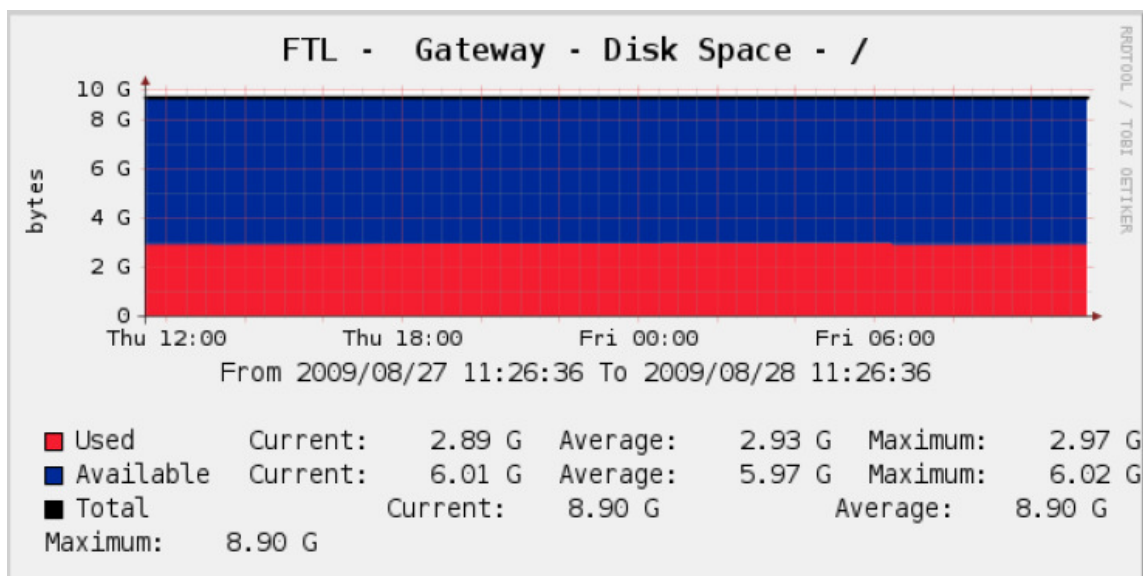


Figura 15 – Gráfico de espaço em disco de um equipamento de um cliente

Na figura 16 é apresentado o gráfico de utilização de CPU do equipamento monitorado. Pode-se ver claramente um picos na utilização de CPU por volta das 00:00 hs e das 06:00 hs da manhã. É função do administrador conhecer o comportamento dos equipamentos de rede para que, ao olhar esses gráficos, ele veja se este comportamento está correto ou está ocorrendo algum problema.

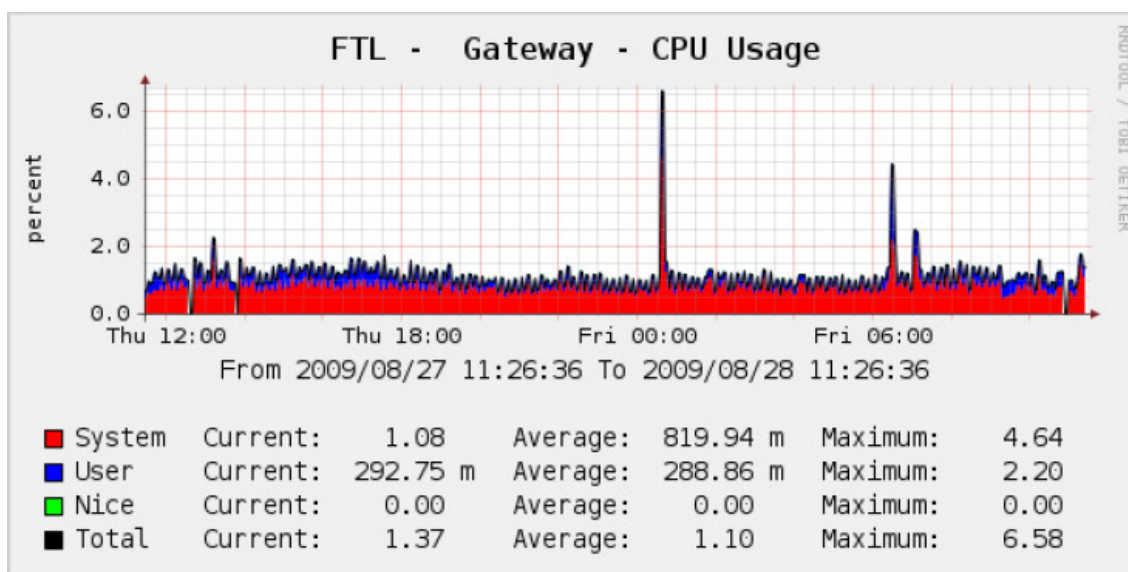


Figura 16 – Gráfico de utilização de CPU por um equipamento de um cliente

3.1.3 Exemplo de relatório sobre monitoramento mensal de cliente

Abaixo temos um relatório elaborado pela equipe de suporte da Huthil Tecnologia que é apresentado mensalmente a cada um dos seus clientes. Neste relatório são informados as estatísticas e alertas dos servidores e serviços das redes destes clientes, de modo a mostrar-lhes que o SLA (Service Level Agreement) acordado em contrato foi ou não atingido. Vale ressaltar que essas informações fornecidas neste relatório foram levantadas e retiradas das ferramentas Nagios e Cacti.

Na página 1 (figura 17) é apresentado o objetivo do relatório, suas metas e alertas de não conformidade, durante o mês, encontrados pela equipe de suporte.

Parecer Técnico Mensal

sexta-feira, 28 de agosto de 2009
15:50



Infraestrutura de rede de computadores - Equipamentos / Serviços Supervisionados

Empresa: Fastel do Brasil

Período: 15/07 - 15/08/2009

Objetivo

Apresentar estatísticas dos servidores e serviços da rede de computadores supervisionados pela Huthil Tecnologia, em conformidade ao contrato de serviços firmado entre as partes.

Local

Av. Presidente Dutra 2480 - Pavuna - Rio de Janeiro - RJ.

Metas

- Confirmação do escopo de equipamentos / serviços em supervisão
- Apresentação do índice de disponibilidade dos equipamentos / serviços supervisionados e descrição dos eventuais problemas
- Alertas (situações em não conformidade)

Confidencialidade

- Este documento possui informações confidenciais e destina-se exclusivamente à Fastel, com cópia parcial ou total de seu conteúdo proibida.

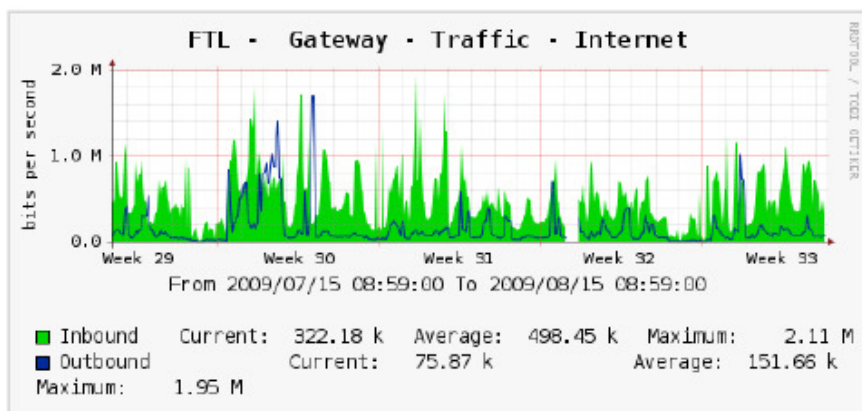
Alertas

- **Não conformidade: Servidor FSTSBS01 sem garantia do fabricante**
 - Problema: Impossibilidade de ações preventivas de hardware.
 - Problema: Serviços hospedados na máquina ameaçados em caso de falha de hardware, pois as peças de substituição somente são conseguidas junto ao fabricante. Tempo de retorno dos serviços sem garantia de tempo definido.
 - **Solução: Aquisição junto ao fornecedor dos servidores de extensão de garantia.**
- **Não conformidade: Servidor FSTSBS01 sem Antivírus**
 - Problema: Impossibilidade de retirada de vírus. Problemas como estes podem gerar a paralisação de serviços essenciais da rede e conseqüente geração de indisponibilidade sem previsão de retorno.
 - **Solução: Aquisição de aplicativo de antivírus corporativo.**
- **Não conformidade: Servidor FSTSBS01 com alto índice de processamento**
 - Problema: Aplicativos hospedados no servidor com performance prejudicada.
 - **Solução: Migração do sistema com base de dados MySQL para outro servidor.**

Figura 17 – Relatório Mensal – pag. 1

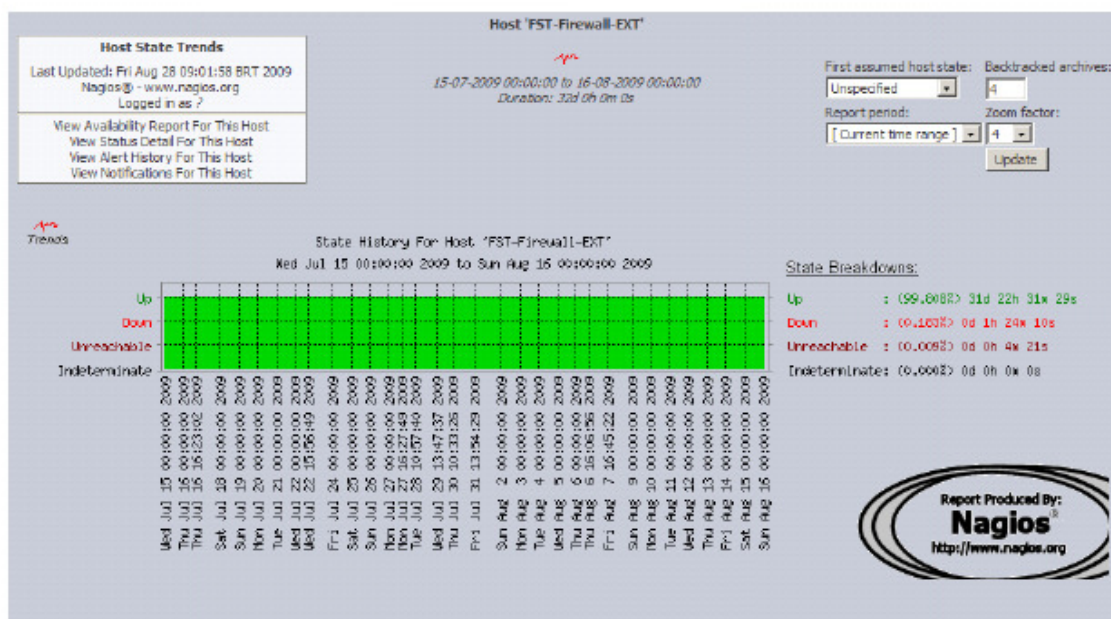
Ná página 2 (figura 18) são apresentados os gráficos de tráfego de acesso a internet (retirado do Cacti) e a disponibilidade do servidor de firewall deste cliente (retirado do Nagios).

LINK INTERNET



Comentários:
Atividade normal para o período.

FSTLNX01

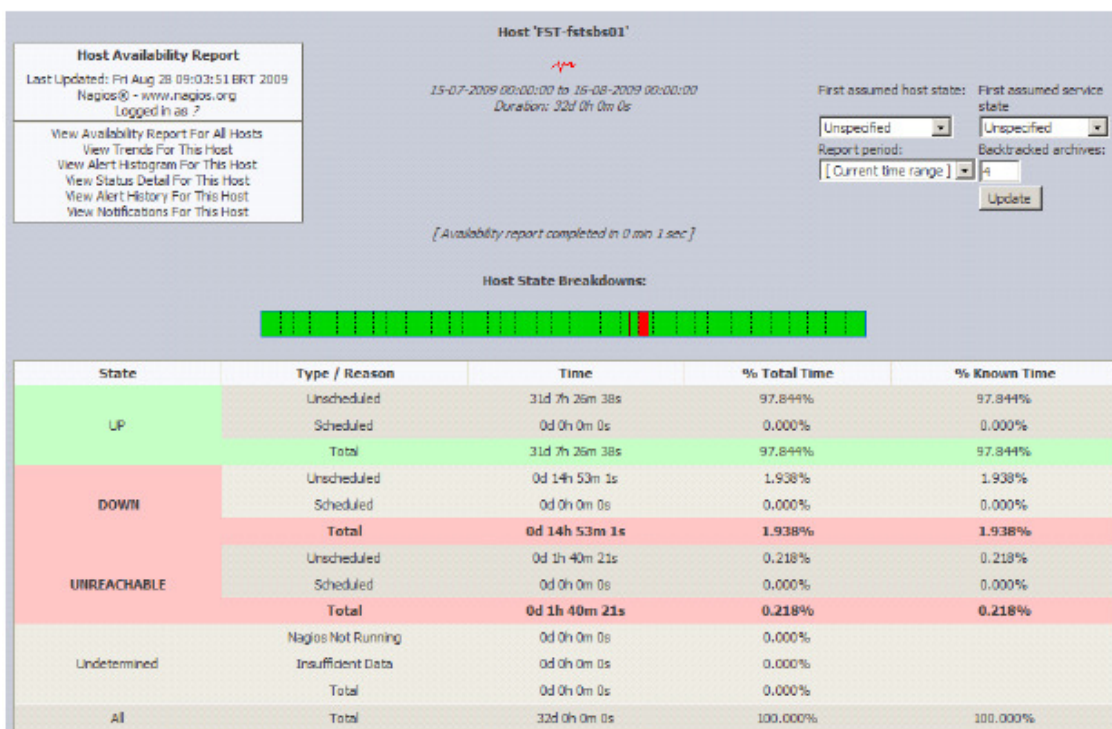


Comentários:
Sem comentários.

Figura 18 – Relatório Mensal – pag. 2

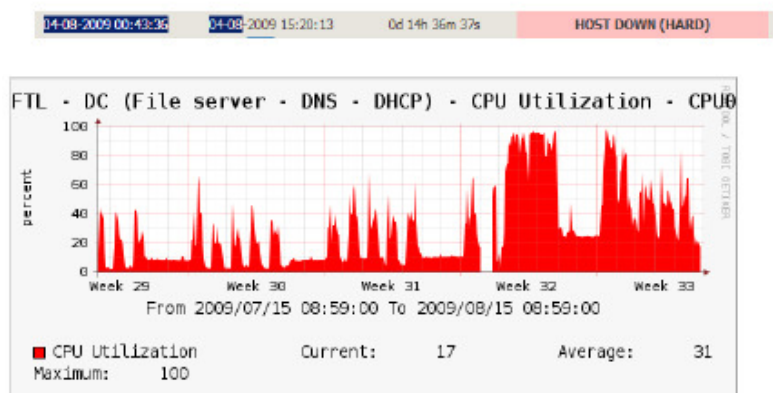
Na página 3 (figura 19) são apresentados os gráficos de disponibilidade do servidor de arquivos (retirado do Nagios) e da carga de CPU deste equipamento (retirado do Cacti).

FSTSBS01



Comentários:

O período de indisponibilidade verificado (04/08) não corresponde à downtime deste servidor (FSTSBS01), estando relacionado à problema verificado no link da Embratel, impossibilitando a ação de monitoramento.



Comentários:

Observado alto índice de processamento referente ao sistema com base MySQL, principalmente nas semanas 32 e 33.

Figura 19 – Relatório Mensal – pag. 3

3.2 GOLDEN CROSS

É uma empresa no ramo de saúde que atua no mercado há mais de 20 anos sendo uma das líderes neste segmento.

O Departamento de Infra-estrutura (DEINF) é o responsável pela manutenção e administração de todos os recursos de TI da empresa (computadores, notebooks, servidores, switches, roteadores, links, telefonia, Voip, etc.).

O CPD da Golden Cross, sob a responsabilidade deste departamento, é formado por vários servidores físicos Windows, Linux (Red-Hat Enterprise), e servidores VMWare Infraestructure 3 configurados em cluster (hospedando servidores Windows e Linux virtualizados), servidores RISC rodando HP-UX (servidores de missão crítica) e dois storages HP (um com 4 Terabytes e outro com 15 Terabytes), operando em regime 24 x 7 (24 horas por dia, 7 dias por semana), visando atender aos serviços de email (Lotus Notes / Domino), aplicações (Websphere, Jboss, PeopleSoft), acesso remoto (Citrix Metaframe) e bancos de dados (Oracle e Sybase)

O monitoramento de todo este parque de máquinas é responsabilidade da equipe de suporte a servidores do departamento de infra-estrutura e para tal é utilizado o software Big Brother. Além disso essa equipe também mantém o histórico de inventário, alterações dos sistemas (Relatórios de Requisição de Mudaças) e relatórios de falhas ocorridas (Relatório de Incidentes).

Cada serviço possui um SLA que foi acordado durante o processo de homologação do mesmo. Quando ocorre uma parada não programada (falha) em algum serviço, a equipe de suporte parte imediatamente para a solução do problema a fim de reiniciar o serviço dentro do SLA acordado. Após a solução deste serviço um relatório (Relatório de Incidentes) deve ser encaminhado para a gerência do departamento, informando a causa do problema, a solução utilizada e as áreas afetadas pela parada desse serviço.

Quando é necessário parar algum serviço da rede para manutenção ou atualização de produto é necessário outro relatório (Formulário de Requisição de Mudanças), onde será explicado o motivo da parada, as ações que serão efetuadas para a mudança e uma análise de risco sobre essa mudança e como se dará o *fallback* (retorno às condições de funcionamento antes da mudança) em caso de problemas. Esse relatório deve ser encaminhado para a gerência do departamento

de infra-estrutura e somente após a aprovação dos gerentes de todas as áreas envolvidas no processo a mudança poderá ser realizada.

3.2.1 Monitoramento pela Ferramenta Big Brother

O Big Brother [15], através de sua interface Web, mostra informações sobre o comportamento dos serviços e equipamentos monitorados em uma matriz de pontos coloridos. Os pontos verdes indicam os processos normais, os amarelos indicam alertas e os vermelhos indicam que algum serviço ou equipamento encontra-se com problemas. A cor de fundo da tela de monitoramento do Big Brother sempre indica a cor da condição mais séria dos elementos monitorados.

Além de suporte ao SNMP através de plugins, o Big Brother possui um agente (BB Client) para ser instalado nos equipamentos monitorados que enviará periodicamente ao servidor do Big Brother as informações sobre CPU, processos, espaço em disco e etc. Cada informação enviada possui data e hora de expiração, que permite saber quando a informação não é mais válida.

O Big Brother também possui relatórios que permitem determinar se o SLA de algum equipamento ou serviço está sendo atendido, além de prover acesso ao histórico de informações que permite verificar um problema em qualquer tempo.

A seguir seguem algumas telas onde informações dos equipamentos são apresentadas: na figura 20 é apresentada a última informação da utilização de CPU informada pelo agente do servidor PSPRD01MTZ. Note que há um faixa em verde do lado esquerdo da tela indicando que atualmente este serviço não apresenta nenhum alerta. Na figura 21 é apresentada a utilização dos discos deste mesmo servidor. Já na figura 22 é apresentada a utilização de disco de outro servidor, mas com alerta informando que o disco *K* já está alertando em nível crítico (*PANIC level*), e os discos *N* e *S* estão apenas alertando que o disco está em nível de alerta (*WARNING Level*)

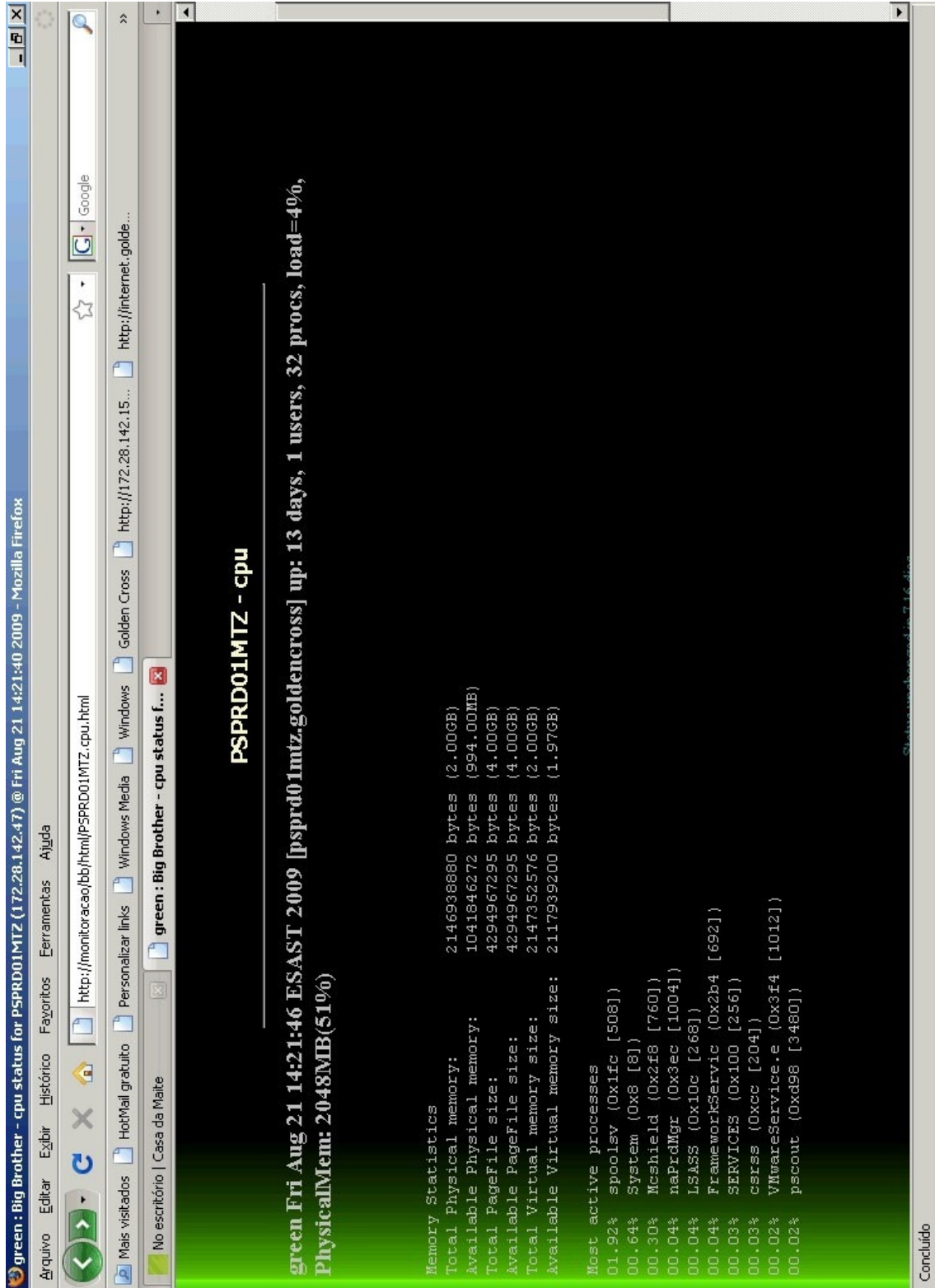


Figura 20 – Utilização de CPU de equipamento

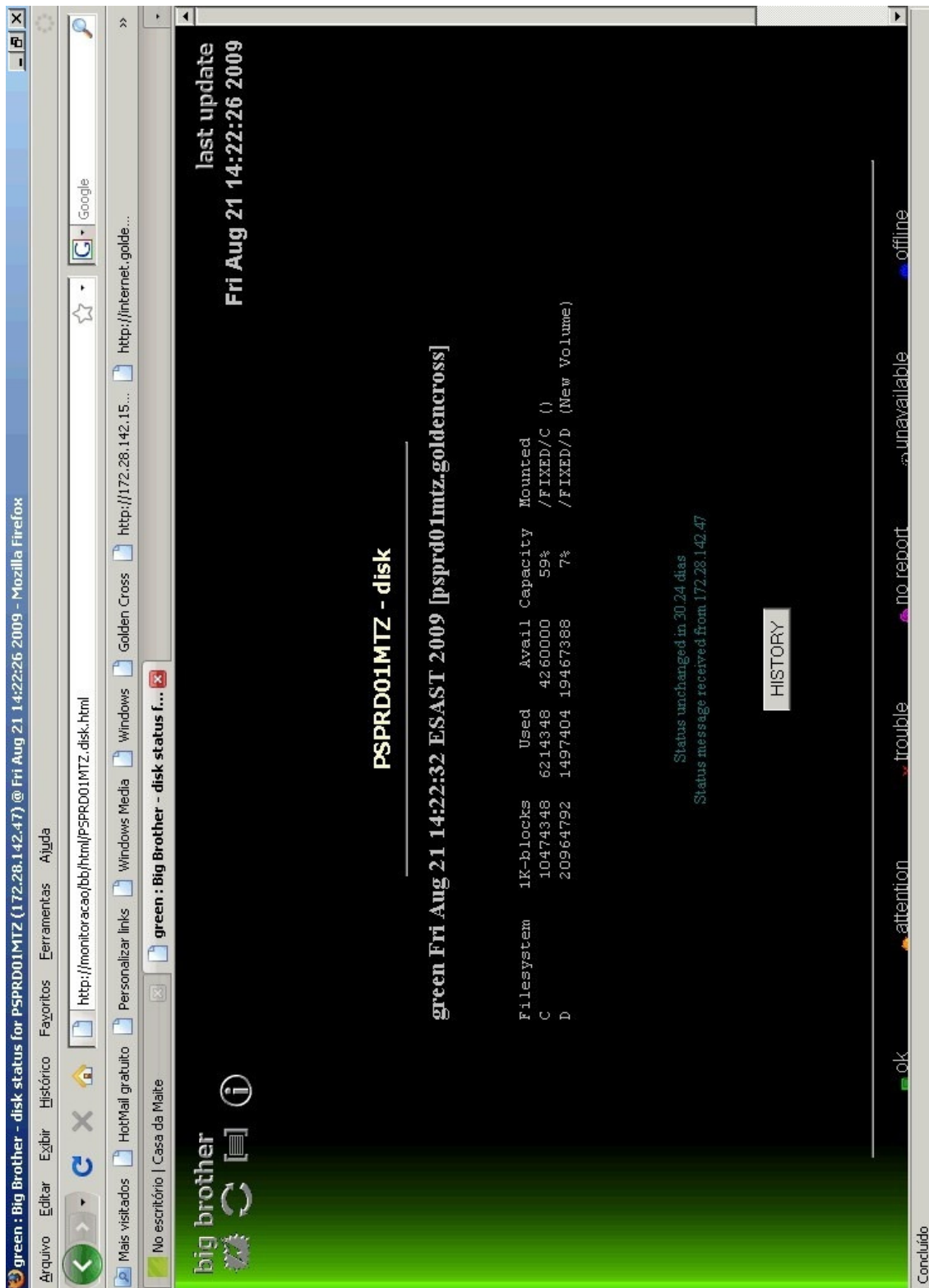


Figura 21 – Utilização de disco de um equipamento

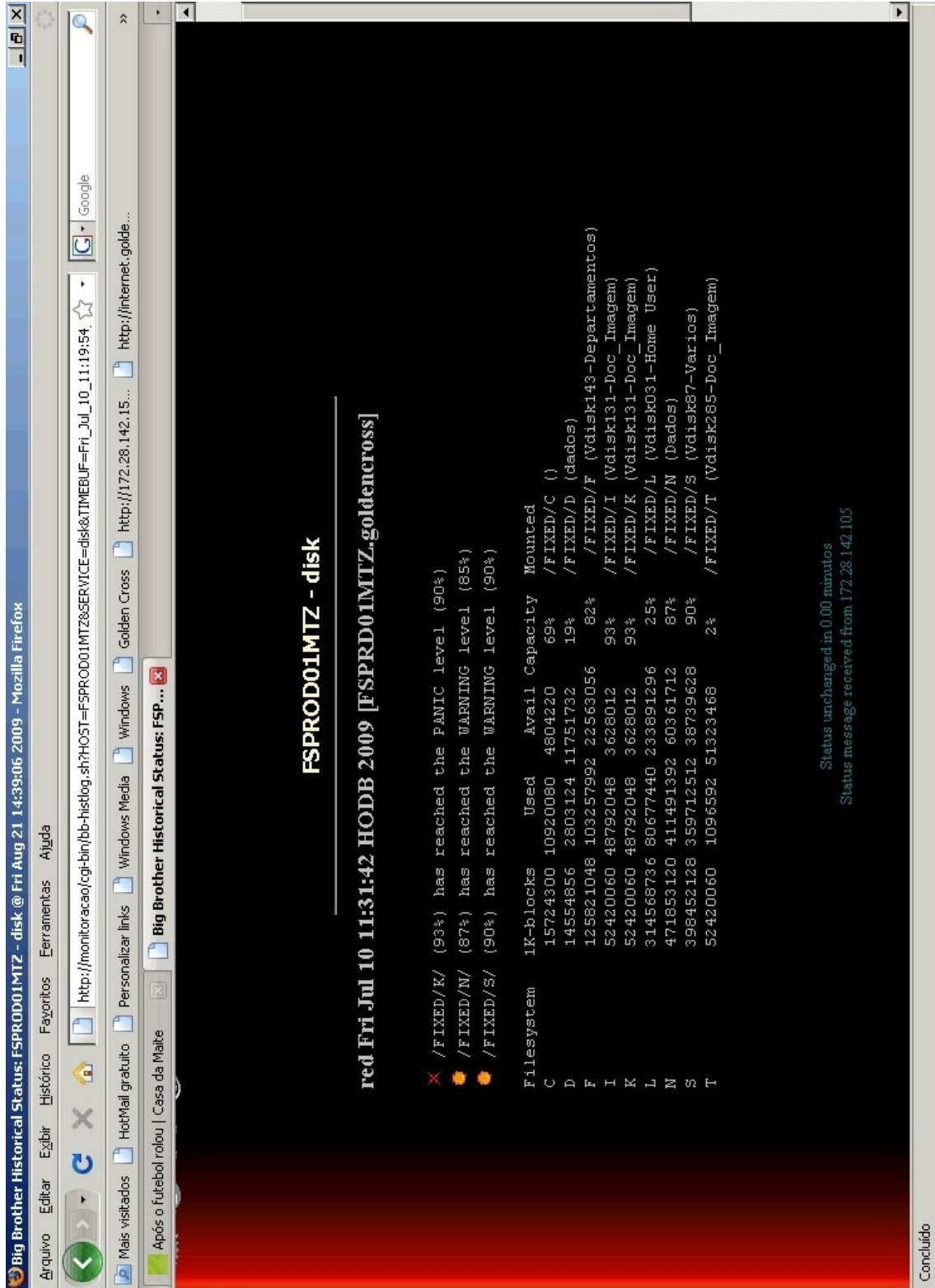


Figura 22 – Utilização de disco de um equipamento

3.2.2 Exemplo de Formulário de Requisição de Mudanças

Abaixo temos um formulário onde é feita a requisição de uma mudança no ambiente de produção do CPD. Este formulário tem por finalidade principal documentar todas e quaisquer alterações executadas nos servidores e equipamentos de rede, facilitando em muito a rastreabilidade de qualquer incidente originado por uma alteração neste ambiente.

Este relatório é formado por 4 partes: Na primeira parte é apresentada a mudança, a motivação que levou a executá-la, as pessoas e recursos envolvidos, que serviços serão afetados durante esta mudança e a sua duração estimada.

Na segunda parte são apresentados os detalhes técnicos, como uma descrição mais detalhada da mudança, uma tabela das atividades a serem executadas e uma análise de risco. Essa análise de risco deve levar em conta o “*fallback*”, isto é, o retorno da condição original, caso a mudança ocasione algum outro incidente não previsto e que não seja de rápida solução.

Na terceira parte são descritos os testes a serem realizados para a verificação do sucesso da mudança, seus procedimentos, resultados esperados em cada teste, as tolerâncias a erros que possam ocorrer e quem irá validar o teste.

A quarta parte se destina às aprovações, isto é, quem elaborou, verificou e aprovou a execução desta mudança.

 Golden Cross	Formulário de Requisição de Mudança (FRM)
SUTIN	

Solicitante	André Gheventer
Área	DEINF
Telefone	XXXX-4022

1. Especificação Funcional

Descrição da Mudança / Escopo Geral:
Análise do problema de lentidão Barracuda.

Áreas / Recursos envolvidos na execução da mudança
DEINF / Suporte de TI – Wagner Freitas
OpenNet – Flavio e Junior

Serviços afetados
Nenhum serviço será impactado.

Data e hora previstas / Tempo Estimado
Data: 10/09/2009.
Início: 19:30
Tempo previsto: 30 minutos

2. Especificação Técnica

Descrição:
Análise do problema de lentidão no acesso ao console Barracuda.

2.1 Tabela de Atividades

Atividade	Responsável	Data-Hora Início	Data-Hora Fim
<i>Alteração das opções de Quarentena que estavam desabilitadas</i>	OpenNet – Flavio DEINF – Wagner Freitas	<i>10/09/2009 19:30</i>	<i>10/09/2009 19:45</i>
<i>Executar testes de entrada/saída de mensagens.</i>	OpenNet – Flavio DEINF – Wagner Freitas	<i>10/09/2009 19:45</i>	<i>10/09/2009 20:30</i>

2.2 Análise de Risco

	Descrição	Probabilidade (Alta, Média, Baixa)	Impacto (Alto, Médio, Baixo)	Ação de Contorno
1	<i>Não é possível remover a entrada no Barracuda.</i>	<i>B</i>	<i>B</i>	<ul style="list-style-type: none"> <i>Verificar motivo e solucionar problema junto ao suporte Barracuda.</i>
2	<i>Detectado problemas no envio ou recebimento de mensagens</i>	<i>B</i>	<i>A</i>	<ul style="list-style-type: none"> <i>Adicionar a entrada goldencross.com.br, ou seja desfazer o procedimento.</i>

3. Ambiente de Teste

-	Teste de envio e recebimento de mensagens.
---	--

Procedimento de Teste	Análise do comportamento do Barracuda após a alteração.
Resultado Esperado	Funcionamento do roteamento de mensagens.
Tolerância	Não se aplica
Validado por	DEINF – Wagner Freitas OpenNet – Flavio e Junior
Comentários	Caso não se obtenha o resultado esperado, verificar ações de contorno relatados na seção 2.2 (item 2) - Análise de Risco.


4. Aprovações

Elaborado por:	<i>Wagner Freitas</i>
Validado por:	<i>Marcilio Calado</i>
Aprovado por:	<i>André Gheventer</i>

3.2.3 Exemplo de Relatório de Incidente

Abaixo temos um formulário onde é feito o relato da ocorrência de um incidente em qualquer serviço ou servidor do ambiente de produção. Este documento tem por finalidade documentar e criar um histórico dos incidentes ocorridos, facilitando uma solução mais rápida quando ocorrem incidentes iguais, pois o conhecimento para a aplicação de uma solução já se encontra pronta.

Neste relatório são informadas a descrição básica do incidente e outra mais detalhada, o período de ocorrência deste incidente, as pessoas envolvidas na sua solução, que impactos foram gerados, quais as ações tomadas para finalizar o incidente e uma conclusão informando se o incidente foi resolvido, ou se este incidente gerou ou irá gerar uma mudança. Quando isso acontece, deve-se informar o número do relatório de mudança associado a esse evento.

	Relatório Ocorrência de Problemas	DEINF SUTIN
---	--	------------------------

Descrição do Problema

Ambiente do VPO ficou extremamente lento durante o dia.

Data: 08/09/2009 - Hora inicio: 10:00 h

Data: 08/09/2009 - Hora termino: 15:10 h

Áreas e pessoas da SUTIN envolvidas

Nome	Área	Telefone/Ramal
Bruno Pereira	DEINF	2711
Marcilio Calado	DEINF	2092

Descrição detalhada do problema

Após contato feito pela Eliandra - DEQTI, foi verificado que o ambiente do VPO estava muito lento. Foi detectado no servidor que o processo do MySQL estava consumindo 99% de cpu.

Ao analisar a lista de processos ativos no banco de dados, não foi possível detectar a sessão causadora da contenção. Fora isso, haviam sessões antigas presas. Devido aos fatos fomos indicados a executar um boot do servidor.

Impactos no negócio

O VPO ficou indisponível no momento do boot (15:00 – 15:10).

Ações Corretivas

Efetuar o boot no servidor vpoprd01mtz.

Conclusão

Após o boot o ambiente foi normalizado ficando disponível e com boa performance para acesso.

4 CONCLUSÃO

Como dito na introdução, com a crescente complexidade das redes de computadores, um sistema de gerenciamento de redes torna-se cada vez mais indispensável. Somente com o auxílio de ferramentas é possível enxergar mais precisamente o que acontece no interior de uma rede de computadores.

As ferramentas de gerenciamento são capazes de fotografar áreas e elementos internos de uma rede, revelando ao administrador focos que requerem sua intervenção ou simplesmente tranquilizando-o pelo fato de que tudo está funcionando perfeitamente em um dado momento.

Uma solução de gerência implantada em uma rede antes desprovida deste serviço eleva significativamente o padrão de qualidade do trabalho do administrador da rede. Faz isso por diminuir o tempo de detecção de falhas, auxiliar pró-ativamente na detecção de gargalos, manter histórico de contabilização de recursos, de disponibilidade e de tendências, e por permitir ao administrador ter uma visão precisa e centralizada de todos os elementos importantes da rede.

5 REFERÊNCIAS BIBLIOGRÁFICAS

- [1] J. Case, M. Fedor, M. Schoffstall, J. Davin, IETF RFC 1157: A Simple Network Management Protocol (SNMP). (<http://www.ietf.org/rfc/rfc1157.txt> acessado em Março de 2007).
- [2] M. Rose, K. McCloghrie. IETF RFC 1066: Management Information Base for Network Management of TCP/IP-base Internets. (<http://www.ietf.org/rfc/rfc1066.txt> acessado em Março de 2007).
- [3] K. McCloghrie, M. Rose. IETF RFC 1213: Management Information Base for Network Management of TCP/IP-base Internets: MIB-II. (<http://www.ietf.org/rfc/rfc1213.txt> acessado em Março 2007).
- [4] M. Rose, K. McCloghrie. IETF RFC 1155: Structure and Identification of Management Information for TCP/IP-based Internets. (<http://www.ietf.org/rfc/rfc1155.txt> acessado em Março de 2007).
- [5] J. Case, K. McCloghrie, M. Rose. IETF RFC 1901: Introduction to Community-based SNMPv2. (<http://www.ietf.org/rfc/rfc1901.txt> acessado em Março de 2007).
- [6] J. Case, K. McCloghrie, M. Rose. IETF RFC 1902: Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2). (<http://www.ietf.org/rfc/rfc1902.txt> acessado em Março de 2007).
- [7] J. Case, K. McCloghrie, M. Rose. IETF RFC 1903: Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2). (<http://www.ietf.org/rfc/rfc1903.txt> acessado em Março de 2007).
- [8] J. Case, K. McCloghrie, M. Rose. IETF RFC 1904: Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2). (<http://www.ietf.org/rfc/rfc1904.txt> acessado em Março de 2007).
- [9] J. Case, K. McCloghrie, M. Rose. IETF RFC 1905: Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2). (<http://www.ietf.org/rfc/rfc1905.txt> acessado em Março de 2007).
- [10] J. Case, K. McCloghrie, M. Rose. IETF RFC 1906: Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2). (<http://www.ietf.org/rfc/rfc1906.txt> acessado em Março de 2007).
- [11] J. Case, K. McCloghrie, M. Rose. IETF RFC 1907: Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2). (<http://www.ietf.org/rfc/rfc1907.txt> acessado em Março de 2007).
- [12] J. Case, K. McCloghrie, M. Rose. IETF RFC 1908: Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework. (<http://www.ietf.org/rfc/rfc1908.txt> acessado em Março de 2007).

- [13] Nagios – The Industry Standard in IT Infrastructure Monitoring. (<http://www.nagios.org> acessado em Setembro de 2009).
- [14] Cacti – The complete rrdtool-based graphing solution (<http://www.cacti.net> acessado em Setembro de 2009).
- [15] Big-Brother – Network Monitoring software (<http://bb4.com> acessado em Setembro de 2009).