Monitoramento de Servidores e Envio de Alertas como Prevenção da Indisponibilidade em Ambiente Hospitalar

Fabiano Oliveira dos Santos

Orientador: Diego Fiori de Carvalho

Curso de Sistemas de Informação – Centro Universitário UNIFAFIBE

Bebedouro –SP – Brasil

{sisunifafibe}@unifafibe.com.br

RESUMO

O objetivo deste artigo é demonstrar a importância da utilização de ferramentas de monitoramento, como apoio na prevenção da indisponibilidade de servidores em um ambiente de pronto atendimento hospitalar. No pronto atendimento hospitalar é inadmissível que os registros médicos estejam indisponíveis no ato do atendimento. Por isso, a importância de se manter um sistema íntegro e funcional durante o maior tempo possível para evitar falhas que comprometam a integridade dos dados. Foi realizado pesquisas das principais ferramentas de monitoramento e adotou-se como objeto de estudo e implantação o Zabbix. O monitoramento ocorreu em servidores alocados em um hospital particular, com serviço de pronto atendimento, na cidade de Bebedouro-SP. Com base nos dados coletados, observou-se que, os servidores estão em perfeito funcionamento, mantendo-se dentro do que é esperado para garantir o atendimento no hospital. Porém, identificou-se situações de alerta que necessitam de maior atenção por parte da equipe de TI. Ao final do trabalho, concluiu-se que o monitoramento com envio de alertas é ferramenta fundamental de para auxiliar na gestão da rede, e proporciona benefícios imediatos à equipe técnica e de gestão.

Palavras-chave: Redes. Monitoramento de servidores. Zabbix. Alertas Zabbix

1. INTRODUÇÃO

No ambiente de pronto atendimento hospitalar, a coleta de dados inicia-se com a chegada dos pacientes à recepção e posteriormente a diversas áreas do hospital como triagem, enfermagem, salas de procedimentos, até a área

administrativa, onde ocorre o processamento desses dados que irão compor o prontuário médico dos pacientes. Por isso, a importância de se manter um sistema íntegro e funcional durante o maior tempo possível para evitar falhas que comprometam a integridade dos dados e prejudiquem alguma etapa do processo.

Na visão de ZANON (2001), um dos grandes problemas na qualidade da gestão hospitalar é referente à disponibilidade da informação, onde se faz necessário que os registros médicos, de enfermagem e prontuários dos pacientes estejam sempre acessíveis, inclusive considera inadmissível que os registros médicos estejam indisponíveis no ato do atendimento.

Diante deste contexto é clara a visão de que, para tentar garantir a disponibilidade pelo maior tempo possível, seria necessário o empenho de várias pessoas em um monitoramento contínuo dos ativos da rede.

Segundo ALBUQUERQUE (2001), para contornar este problema, o monitoramento de redes se torna extremamente importante e imprescindível, pois o acesso às informações sobre a saúde dos servidores em tempo real antecipa uma tomada de decisão de forma rápida e confiável. Com o auxílio do *software* apropriado, o esforço para que os servidores operem em pleno funcionamento e sem interrupções não depende mais somente do empenho humano.

O presente artigo buscou demonstrar, por meio da implantação de um *software* de monitoramento e envio de alertas, a importância do monitoramento de servidores como prevenção da indisponibilidade de serviços em um ambiente de pronto atendimento hospitalar.

2. REFERENCIAL TEÓRICO

2.1. Gerenciamento de redes

O gerenciamento ou monitoramento de redes consiste em monitorar as atividades e uso dos recursos da rede, visando garantir a qualidade e disponibilidade dos serviços (LIMA, 2014).

> De acordo com Saydam (1996 apud KUROSE; ROSS, 2006, p.575): *"Gerenciamento de rede inclui o oferecimento, a integração e a coordenação de elementos de hardware,*

> *software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer as exigências operacionais, de desempenho e de qualidade de serviço em tempo real e a um custo razoável".*

Existem três principais componentes em uma arquitetura de gerenciamento de rede: entidade gerenciadora ou gerente, dispositivos gerenciados e um protocolo de gerenciamento.

2.1.1. Monitoramento de serviços

Na visão de LIMA (2014), um serviço, quando é importante, jamais poderá estar indisponível. Ocorrendo um imprevisto, deverá ter contingência de recursos para manter o serviço no ar sem que os clientes percebam que algum problema está acontecendo.

Dentro de tal contexto, LOPES (2003, p. 16) afirma:

> "*Para manter o bom funcionamento de uma rede de computadores é necessário o auxílio de instrumentação adequada: uma ou mais estações de gerência que mostrem o mapa da rede e estatísticas como taxa de erros, de colisões, estado operacional de equipamentos e interfaces, dentre outras; analisadores de protocolos e outras ferramentas de gerência como ping, traceroute e netstat. É preciso também saber utilizar estas ferramentas e saber interpretar os dados de gerência obtidos com elas. Para muitas informações de gerência estabelecemos limiares que, quando ultrapassados, indicam problemas e podem gerar alarmes*".

2.1.2. PROTOCOLO SNMP

O *SNMP* ou Protocolo Simples de Gerencia de Rede, é um protocolo utilizado por *softwares* de gerência de rede para auxiliar no monitoramento e gestão de dispositivos como roteadores, servidores, impressoras, computadores, etc. Atualmente está na terceira versão (*SNMPv3*) e define como uma entidade

gerenciadora se comunica com os agentes, basicamente é responsável pela eficiência de comunicação entre agente e gerente (COMER, 2007).

O agente *SNMP* possui uma tabela de informações que pode ser consultada ou modificada pelo gerente. É possível consultar, por exemplo, o tráfego de rede em um *switch* ou o estado de memória em uma máquina Virtual. Essa tabela é algo semelhante a um dicionário e é composta por *MIB* e *OID,* onde MIB se refere à base de informações e o OID é o identificador único dentro da *MIB* (4LINUX).

2.2. SISTEMAS DE MONITORAMENTO

2.2.1. *CACTI*

O *CACTI* é uma ferramenta que coleta e armazena todas as informações necessárias para criar gráficos em um banco de dados *MySQL*. O *CACTI* pode escalar para um grande número de fontes de dados e gráficos através do uso de modelos. Isso permite a criação de um único gráfico ou modelo de fonte de dados que define qualquer gráfico ou fonte de dados associada a ele. Os modelos de *host* permitem que você defina os recursos de um *host* para que o *CACTI* possa pesquisá-lo e obter informações sobre a adição de um novo *host*. (CACTI.NET).

Tudo isso está envolvido em uma interface intuitiva e fácil de usar que faz sentido para pequenas instalações até redes complexas com milhares de dispositivos. Permite monitorar qualquer dispositivo que tenha compatibilidade com o protocolo *SNMP* (CACTI.NET).

2.2.2. ZABBIX

De acordo com LIMA (2014), o *Zabbix* é um *software* que possui capacidade de monitorar milhares de itens, conta com um sistema intuitivo de gráficos e relatórios, o que facilita a análise dos dados em tempo real. Toda a configuração é realizada por meio de uma *interface web*, ou seja, diretamente no navegador. Permite a criação de ações e o envio de alertas com base em métricas previamente estabelecidas. O *Zabbix* é *opensource*, ou seja, não é necessária aquisição de licença de uso, o que torna o projeto de implantação mais acessível. Permite monitorar dispositivos que tenham suporte ao protocolo *SNMP,* bancos de dados, aplicações e páginas *web*. Contempla todas as funções necessárias para um bom monitoramento da rede, sem a necessidade de *softwares* adicionais, além de

permitir que profissionais com um nível mais avançado de conhecimento possam modificar o código fonte, personalizando conforme sua necessidade.

O *Zabbix* é composto por três principais componentes: ***Zabbix Server*****:** Recebe os dados coletados e faz o envio de alertas**;** ***Zabbix Agent***: Faz a coleta dos dados, é instalado no dispositivo a ser monitorado; ***Interface WEB***: Permite o acesso aos dados monitorados através de relatórios e gráficos. (Zabbix SIA);

3. METODOLOGIA

Para a elaboração deste trabalho realizou-se pesquisas das principais ferramentas de monitoramento e adotou-se como objeto de estudo e implantação o Zabbix, por ser mais completo, permitir criação de mapas de rede, gráficos e envios de alertas sem a necessidade de programas adicionais, e por dispensar a aquisição de licenças, possibilitando uma implantação de baixo custo.

Na instalação do Zabbix, utilizou-se uma máquina virtual com as seguintes configurações: Processador com 2 núcleos, 4 *Gigabytes* de memória e *HD* (*Hard Disk*) de 80 *Gigabyte,* placa de rede *Gigabit* e sistema operacional *Linux Ubuntu* 16. Adotou-se a versão 3.2 do *Zabbix* por ser a mais estável e recente. O processo de instalação do *Zabbix* varia conforme a necessidade, a versão escolhida e o sistema operacional onde será instalado. O tutorial de instalação e configuração pode ser acessado em https://www.zabbix.com/documentation/3.2/pt/manual/installation.

O monitoramento ocorreu em ambiente composto por 9 servidores virtualizados (máquinas virtuais), alocados em um hospital particular de médio porte com serviço de pronto atendimento 24 horas. A escolha dos servidores foi feita com base no nível de criticidade dos serviços, contemplando o mínimo de recursos necessários para manter o hospital em funcionamento.

3.1. Diagrama de funcionamento

Para o monitoramento deve-se instalar o *Agente Zabbix* nos servidores, que fará a coleta dos dados e posteriormente o envio destes ao *Zabbix Server.* Os dados

coletados são analisados pelo *Zabbix Server* e este, ao identificar um incidente, fará o envio do alerta por *e-mail* aos responsáveis pela gestão da rede. A Figura 1, representa o diagrama de funcionamento do *Zabbix,* demonstrando como ocorrerá o processo de coleta de dados e envio de alertas por *e-mail*.

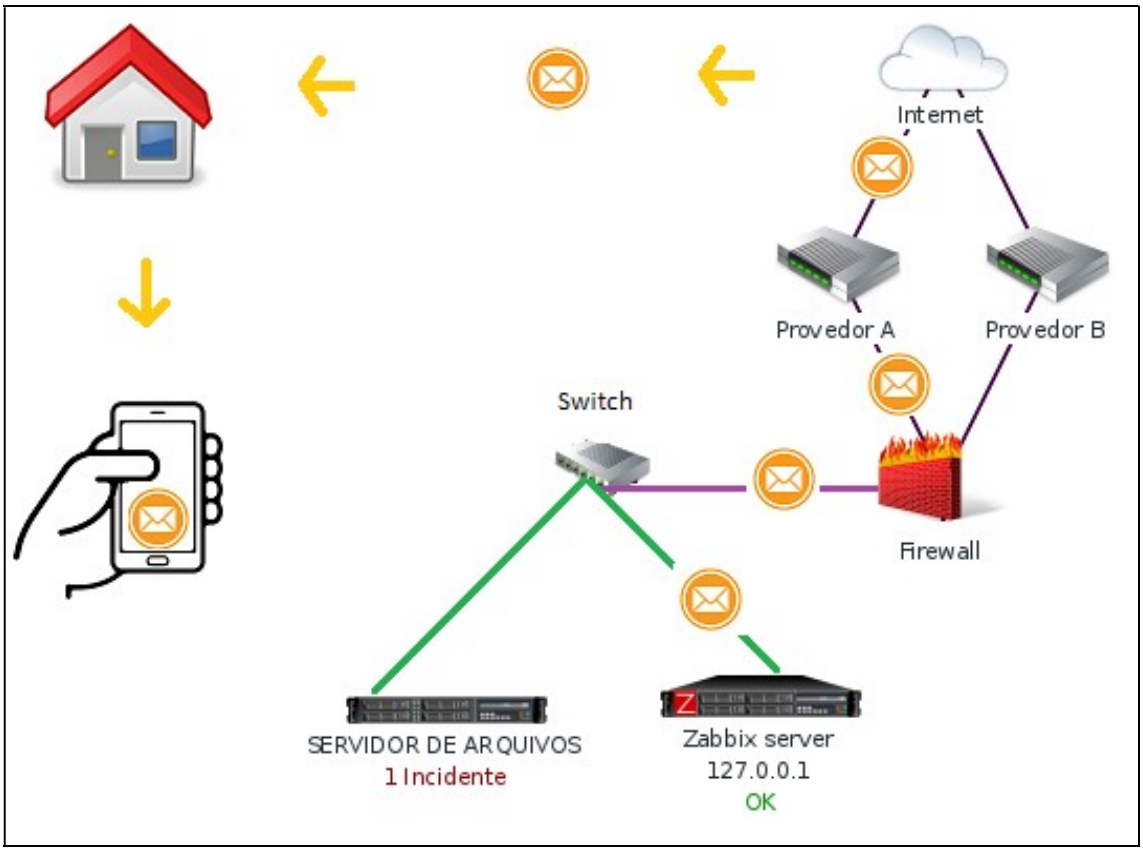

Figura 1. Diagrama de funcionamento (Do Autor).

3.2. Mapa da rede monitorada

É possível ver na Figura 2 o mapa da rede monitorada, que é uma representação gráfica dos servidores monitorados no *Zabbix*. Na criação do mapa da rede os servidores monitorados foram interligados por uma linha verde, que neste caso representa o cabeamento de rede. O mapa da rede é atualizado em tempo real e, quando ocorre algum incidente, a cor da linha é alterada para vermelho e a descrição do incidente é exibida abaixo do servidor monitorado. Os demais itens, interligados com o "cabo de rede" roxo, foram adicionados com a finalidade de ilustrar o caminho por onde os alertas deverão trafegar, via *e-mail*, desde a rede local até a *internet*, onde deverá seguir para entrega ao administrador de redes.

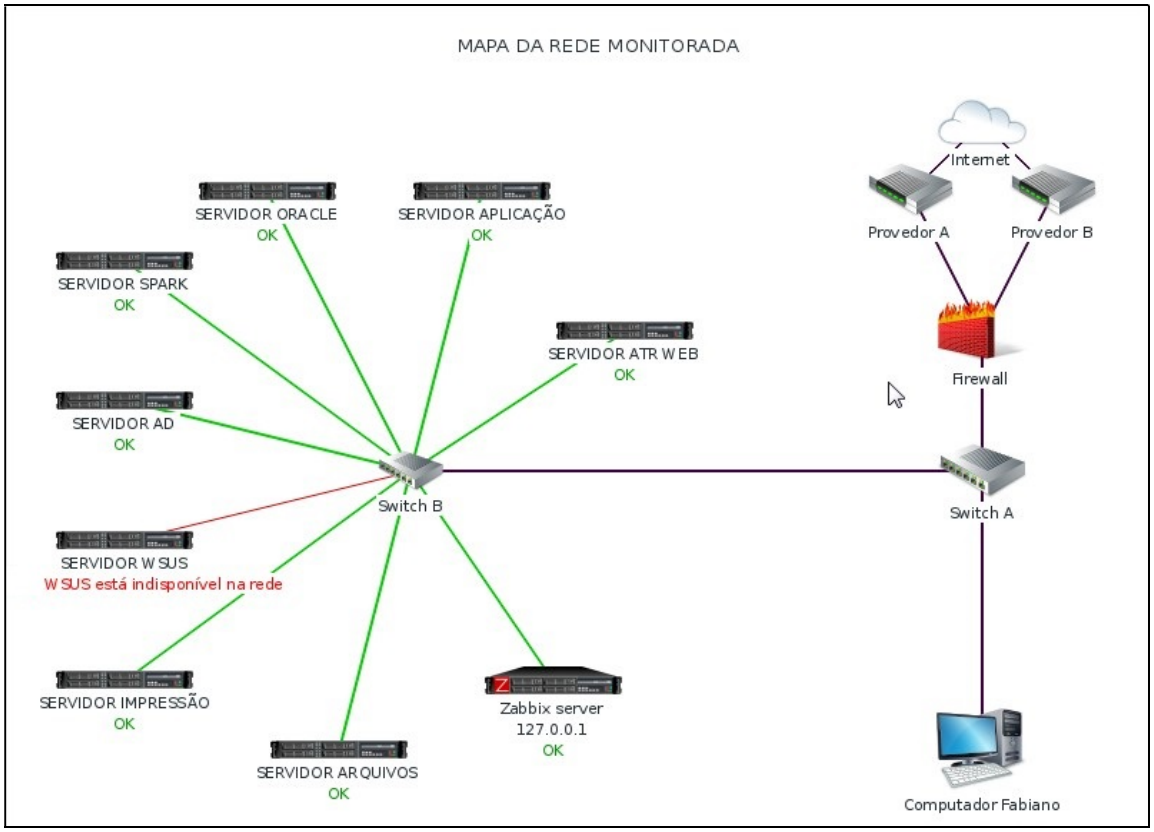

Figura 2. Mapa da rede monitorada (Autor).

3.3. Definindo os parâmetros de monitoramento

Foram adotados como parâmetros de monitoramento quatro dos componentes essenciais ao funcionamento do servidor e definidas métricas que servirão de gatilho para o envio de alertas. Por exemplo, quando o espaço disponível no disco C: atingir 20 *Gigabyte* um alerta de prioridade alta deverá ser disparado. A tabela 1 apresenta os valores que foram definidos pelo coordenador de tecnologia e configurados como parâmetros dos gatilhos de alertas.

RECURSO	CONSUMO DE MEMÓRIA	PROCESSADOR	ESPAÇO LIVRE DISCO C:	ESPAÇO LIVRE DISCO E:	DISPONIBILIDADE
ALERTA PRIORIDADE ALTA	Maior que 90% durante 2 minutos	Maior que 95 % por 2 minutos	Menor que 20 *Gigabyte*	Menor que 10 *Gigabyte*	Quando o servidor desligar, reiniciar ou ficar indisponível na rede por mais de 10 segundos

Tabela 1. Parâmetros para as *Triggers* (gatilhos) de alertas. (Do Autor).

4. DESENVOLVIMENTO

4.1. Configurando a coleta dos dados

O *Zabbix* coleta os dados por meio de um agente *Zabbix* que é instalado no servidor ou utilizando o protocolo *SNMP*. Os agentes são extremamente eficientes, pois utilizam chamadas nativas do sistema operacional para obter as informações estatísticas (ZABBIX SIA, 2017). Desta forma, adotou-se o agente *Zabbix* como coletor de dados.

Para iniciar a coleta de dados é necessário primeiramente adicionar os *hosts* que serão monitorados. No *Zabbix, hosts* são todos os ativos de rede que podem ser monitorados (computadores, servidores, impressoras, etc). A configuração dos *hosts* é feita acessando o menu “Configuração > Hosts > Criar Host”.

A próxima etapa é a criação de *Templates*, que são grupos onde os *Hosts* semelhantes podem ser organizados. Os *Templates* possibilitam também a replicação de uma configuração específica para vários *hosts* simultaneamente.

Após a criação do *Template* adiciona-se o Item, que é o objeto a ser monitorado. Para este trabalho foram definidos os Itens: Uso de processador, Uso de memória, Disponibilidade na rede e Espaço livre em disco. No cadastro de Item são parametrizadas as funções que farão efetivamente a coleta dos dados. A Figura 3, demonstra as funções que foram utilizadas para coleta dos dados.

Nome ▲	Chave
% memória em uso	vm.memory.size[pused]
% memória livre	vm.memory.size[pavailable]
Disponibilidade	icmpping
Espaço em uso disco C:	vfs.fs.size[C:,used]
Espaço em uso disco E:	vfs.fs.size[E:,used]
Espaço livre disco C:	vfs.fs.size[C:,free]
Espaço livre disco E:	vfs.fs.size[E:,free]
Memória total	vm.memory.size[total]
Processador	perf_counter["\238(_Total)\6"]

Figura 3. Funções utilizadas para coleta dos dados (Autor).

A próxima etapa contempla a criação de t*riggers,* que são os gatilhos responsáveis por executar uma determinada ação, neste caso o envio de alertas, caso o item monitorado atinja um limite pré-estabelecido. Elas podem ser construídas utilizando-se funções próprias do *Zabbix,* por exemplo, para a coleta de dados de espaço livre no disco C: utilizou-se a função: *{Maquinas virtuais:vfs.fs.size[C:,free].last(10s)}<20G*, onde **Maquinas virtuais** é o nome do *Template,* **vfs.fs.size[C:,free]** é a função do *Zabbix* que retorna o espaço livre no disco C: **, last(10s)}** refere-se aos últimos 10 segundos de dados coletados e **< 20 G** é o valor em *Gigabyte* que foi atribuído como parâmetro para ativação da *trigger.* Também pode-se utilizar funções próprias do Sistema Operacional, conforme o exemplo de função para a *trigger* Processamento alto: {Maquinas virtuais:perf_counter["\238(_Total)\6"].last(2m)}>95. A Figura 4 demonstra as *Triggers* que foram utilizadas neste projeto.

Nome ▲	Expressão
Consumo de memória	{Maquinas virtuais:vm.memory.size[puse
Espaço livre em disco C: {HOST.NAME}	{Maquinas virtuais:vfs.fs.size[C:,free].las
Espaço livre em disco E: {HOST.NAME}	{Maquinas virtuais:vfs.fs.size[E:,free].las
Processamento alto em {HOST.NAME}	{Maquinas virtuais:perf_counter["\238(_T

Figura 4.*Triggers* configuradas (Do Autor).

Por fim configura-se as ações que serão executadas quando uma trigger for acionada. A Figura 5, contém exemplo das ações que foram cadastradas com base nas *triggers* configuradas anteriormente.

Nome ▲	Condições	Operações
Consumo memória	Severidade da trigger = *Alta* Trigger = *Maquinas virtuais: Consumo de memória*	**Enviar mensagem para o grupo de usuários:**
Disponibilidade	Severidade da trigger = *Alta* Trigger = *Maquinas virtuais: Maquinas virtuais está indisponível na rede*	**Enviar mensagem para o grupo de usuários:**
Espaço em disco C:	Severidade da trigger = *Alta* Trigger = *Maquinas virtuais: Espaço em disco C: Maquinas virtuais*	**Enviar mensagem para o grupo de usuários:**
Uso Processador	Severidade da trigger = *Alta* Trigger = *Maquinas virtuais: Processamento alto em Maquinas virtuais*	**Enviar mensagem para os usuários:** Admin (Z

Figura 5. Ações que serão executadas com base na *trigger*. (Do Autor).

5. RESULTADOS

A Figura 6, apresenta uma representação gráfica do consumo de memória do "SERVIDOR *WSUS*". Foi determinado um limite de 60% na utilização da memória total do servidor. Quando esse limite é ultrapassado a *trigger* é acionada disparando o alerta de incidente por *e-mail* ao administrador da rede.

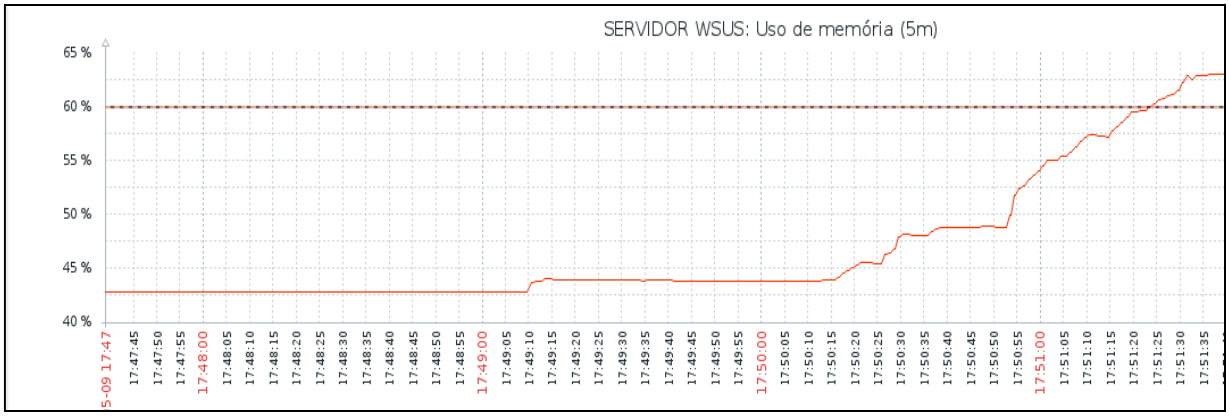

Figura 6. Gráfico de consumo de memória SERVIDOR *WSUS* (Do Autor).

Observando a Figura 7, o gráfico de Uso de memória no período de 7 dias, do "SERVIDOR IMPRESSÃO", apresenta uma constante no uso de memória durante os dias da semana e uma queda acentuada a partir das 0h do dia 15/09/17 (sexta-feira). Com estes dados é possível afirmar, por exemplo, que sexta-feira à noite é o melhor horário para se realizar manutenção preventiva nesse servidor.

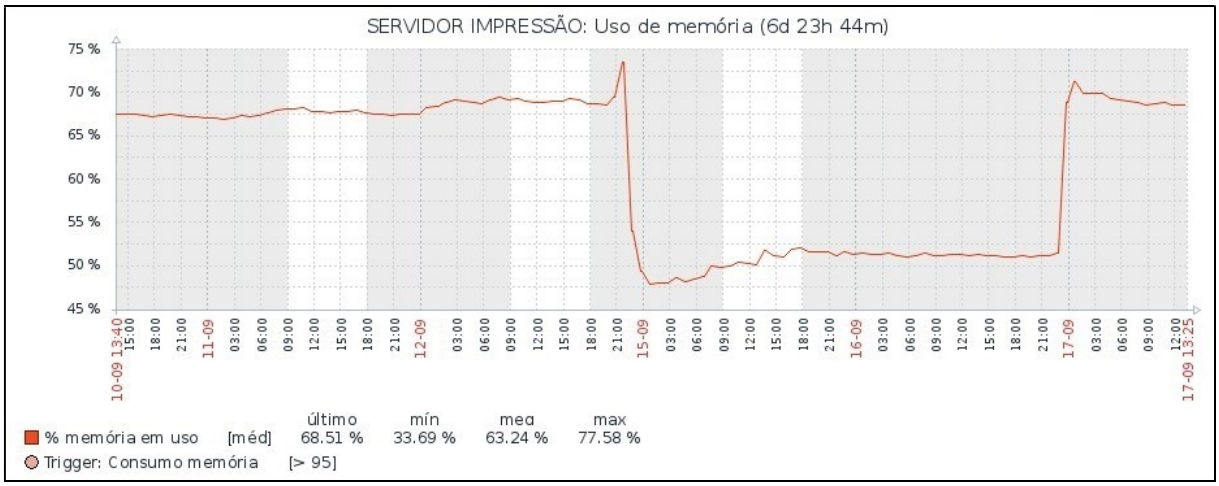

Figura 7. Gráfico de consumo de memória SERVIDOR IMPRESSÃO (Do Autor).

Observa-se na Figura 8 que, em um período de 27 dias, o SERVIDOR APLICAÇÃO teve aumento considerável de uso do processador, inclusive ultrapassando o limite estabelecido, por vários dias e sempre às 12:00. Com base nos dados é possível classificar este como um comportamento anormal, considerando que é o período em que a maioria dos funcionários estão saindo para o almoço e a tendência seria que o processamento fosse mais baixo neste horário.

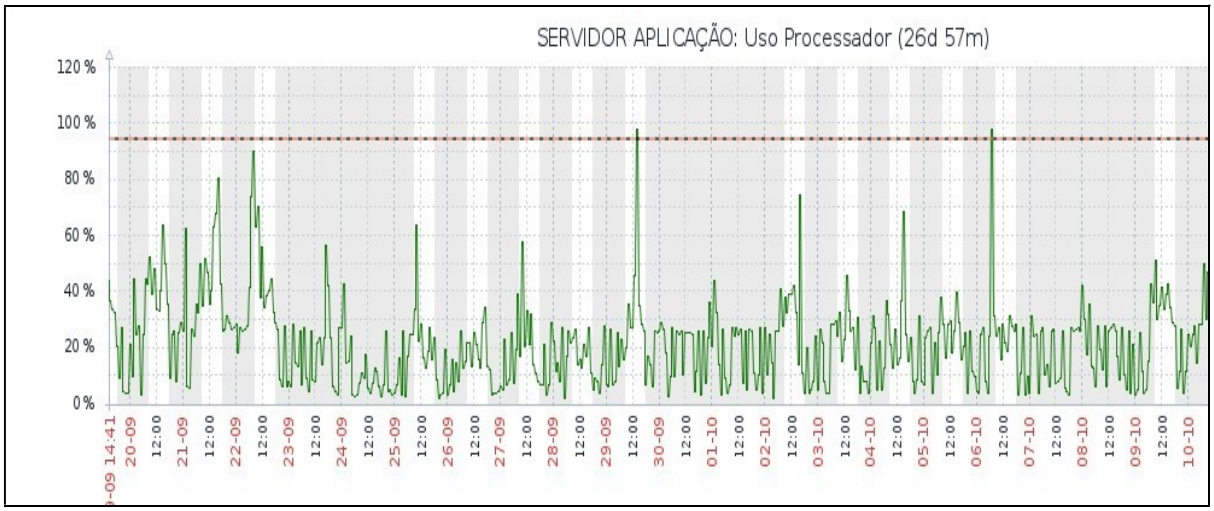

Figura 8. Gráfico Uso de processador SERVIDOR APLICAÇÃO (Do Autor).

A Figura 9 apresenta o gráfico de indisponibilidade do SERVIDOR ORACLE, onde foi registrada uma ocorrência às 16:59 do dia 15/10.

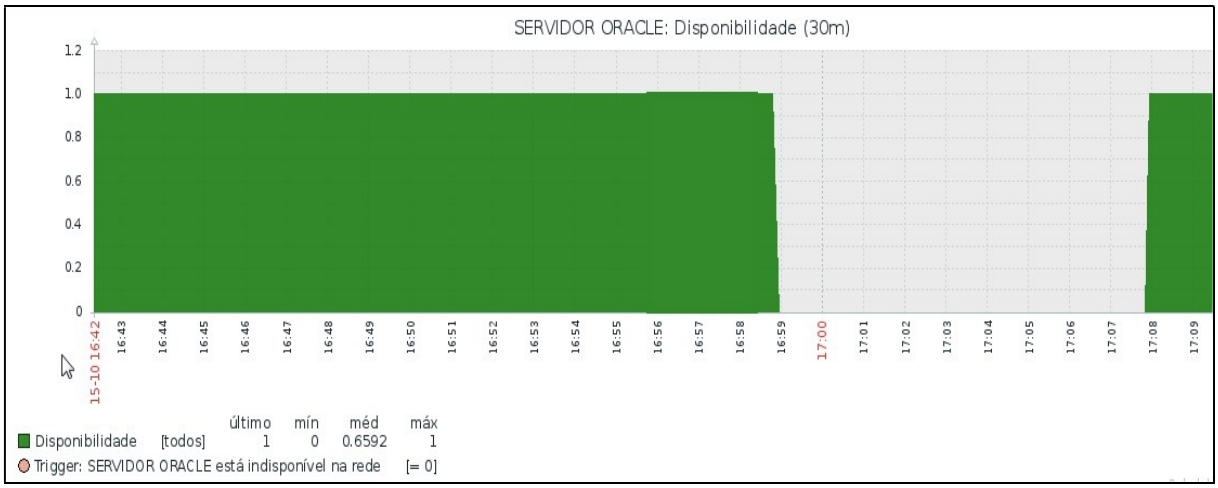

Figura 9. Gráfico de Disponibilidade SERVIDOR ORACLE (Do Autor).

Já a Figura 10, demonstra o alerta de incidente que é enviado por *e-mail* ao administrador de redes. Observa-se que o alerta é enviado imediatamente após o registro do evento pelo *Zabbix*, permitindo que a avaliação do problema seja iniciada o mais breve possível, reduzindo o período de indisponibilidade.

Figura 10. Alerta de indisponibilidade enviado por *e-mail* ao administrador de redes. (Do Autor).

Observa-se na Figura 11 outro exemplo de alerta, enviado quando o espaço disponível no disco C: do SERVIDOR SPARK atingiu 18 *Gigabyte* (a *trigger* é acionada quando este valor é inferior a 20 *Gigabyte*).

Figura 11. Alerta de espaço livre em disco. (Do Autor).

6. CONSIDERAÇÕES FINAIS

Com base nos dados coletados durante o período de elaboração deste artigo, observa-se que não houve grandes períodos de indisponibilidade, mantendo-se dentro do que é esperado para garantir o fluxo de atendimentos no hospital, demonstrando o perfeito funcionamento dos servidores monitorados.

Nota-se, porém, que o SERVIDOR APLICAÇÃO, que hospeda o sistema utilizado pela área administrativa, está trabalhando no limite da sua capacidade de processamento, em um horário que deveria estar ocioso devido à ausência de grande parte dos colaboradores para o intervalo de almoço. Com base nos dados apresentados graficamente pelo *Zabbix*, será possível ao administrador de redes concentrar maior atenção a este servidor e detectar o motivo deste comportamento anormal.

É possível observar ainda que, os dados coletados colaboraram para que se pudesse definir um período de ociosidade dos servidores, que poderá ser aproveitado para as manutenções preventivas, com o mínimo de prejuízo para os atendimentos do hospital. Tais informações seriam praticamente impossíveis de serem obtidas sem o devido monitoramento.

É evidente que o envio de alertas é a peça chave do monitoramento, pois funciona como um vigilante sempre atento que, ao identificar uma falha, notifica

imediatamente os responsáveis, garantindo o menor tempo possível para o início da análise e resolução do problema.

Por fim, conclui-se que o monitoramento é uma ferramenta fundamental e de extrema importância para auxiliar na gestão da rede. Proporciona benefícios imediatos que podem ser aproveitados pela equipe técnica e de gerencia de tecnologia, permite facilmente, por meio da avaliação dos dados gráficos, se antecipar aos problemas, programar as manutenções preventivas e receber alertas por *e-mail* no momento exato da ocorrência de um incidente, podendo iniciar, de forma mais pró ativa, a manutenção daquele servidor para minimizar o período de indisponibilidade, bem como oferecer relatórios gerenciais mais assertivos que possam auxiliar a tomada de decisão sobre investimentos que por ventura precisem ser efetuados para a melhoria contínua dos serviços. Como trabalhos futuros podemos citar a expansão das ações de monitoramento para outros serviços da instituição e a criação de novos gatilhos (*triggers*) para outras ações.

REFERÊNCIAS

ALBUQUERQUE, F. TCP-IP Internet: protocolos & tecnologias**. 3. ed. Rio de Janeiro: Axcel Books do Brasil, 2001.**

4Linux. O que é SNMP. **Disponível em: http://www.4linux.com.br/o-que-e-snmp. Acesso em: 06 de maio de 2015.**

CACTI. About Cacti**. Disponível em: http://www.cacti.net. Acesso em 09 de maio de 2015.**

COMER, Douglas E. Redes de computadores e internet**. 4. ed. Porto Alegre: Bookman, 2007.**

CONTINUUM MANAGED SERVICES LLC. What is a Network Operations Center (NOC)?**. Disponível em: http://www.continuum.net/msp-resources/mspedia/what-is-a-network-operations-center-noc. Acessado em 05 de maio de 2015.**

KUROSE, James F. ; ROSS, Keith W.. Redes de computadores e a internet**: uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.**

KUROSE, James F. ; ROSS, Keith W.. **Redes de computadores e a internet**: uma abordagem top-down. 5 ed. São Paulo: Pearson Addison Wesley, 2010

LIMA, Janssen dos Reis. **Monitoramento de redes com Zabbix**: monitore a saúde dos servidores e equipamentos. Rio de Janeiro: Brasport, 2014.

LOPES, Raquel V. et al. **Melhores Práticas para Gerência de Redes de Computadores**. Rio de Janeiro: Campus, 2003.

MAIA, Luiz Paulo. **Arquitetura de redes de computadores**. 2. ed. Rio de Janeiro: LTC, 2013.

STEFANINI. **NOC – Network Operation Center.** Disponível em: http://stefanini.com/br/2013/10/noc-network-operation-center/. Acesso em 05 de maio de 2015

ZABBIX SIA**. Documentação do Zabbix em Português**. Disponível em: https://www.zabbix.com/documentation/3.2/pt/start. Acesso em 26 de agosto de 2017.

ZANON, Uriel. **Qualidade da assistência médico-hospitalar**. 1. ed. Rio de Janeiro: Guanabara Koogan, 2001.