Gerenciamento e Controle por Autenticação para Acesso à Estrutura de Rede de Computadores da Prefeitura Municipal de Palmeira das Missões – RS

Lázaro Hahn Martins[1], Sidnei Renato Silveira[2], Fernando Beux dos Santos[3]

[1]Curso de Bacharelado em Sistemas de Informação, [2]Departamento de Tecnologia da Informação – Universidade Federal de Santa Maria (UFSM/Campus Frederico Westphalen) – RS – Brasil
[3]Prefeitura Municipal de Palmeira das Missões - RS

lazarohahn@hotmail.com, sidneirenato.silveira@gmail.com, fernandobeux@gmail.com

Resumo. *Este artigo apresenta um estudo de caso envolvendo a implantação de um método para controlar e gerenciar a conexão dos usuários ao acesso à estrutura de rede de computadores da Prefeitura Municipal de Palmeira das Missões – RS (PMPM-RS). Desenvolveu-se um meio de controle e gerenciamento por autenticação, para controlar o acesso à estrutura de rede de computadores.*

Palavras-Chave: Rede de computadores; VLANs; *Hotspot*.

Abstract. *This paper presents a case study of the implementation of a method to control and manage the connection of users to access the computer network structure of the Palmeira das Missões city - RS (PMPM-RS). Thus, a means of control and management for authentication will be developed to control access to the computer network structure.*

Keywords: *Computer network; VLANs; Hot spot.*

1. Introdução

Atualmente, a utilização de ferramentas informatizadas é imprescindível em todos os setores de atividades, tais como os órgãos públicos. As organizações estão, cada vez mais, dependentes de ferramentas tecnológicas e do acesso a informações disponíveis em suas redes internas (Intranet) e na Internet. Neste sentido, gerenciar o acesso à rede e às informações disponíveis passa a ser uma tarefa importante para garantir a segurança e integridade das informações.

A motivação para o desenvolvimento deste trabalho surgiu a partir das atividades exercidas no setor de informática na PMPM-RS (Prefeitura Municipal de Palmeira das Missões-RS), onde os autores deste trabalho atuam. Constatou-se, durante o desenvolvimento destas atividades, fragilidade na questão de segurança dos acessos dos usuários, nas pessoas que possuem acesso à rede (com a falta de identidade dos usuários em seus acessos) e, também, na quantidade de vírus que se espalham nos computadores tanto por descuido, como na questão de falta de comprometimento com o trabalho exercido nos setores. Além disso, havia necessidade em diminuir o tráfego na rede, pois

a demanda de acessos a conteúdos que não fazem parte do trabalho desenvolvido pelos servidores públicos era excessiva.

Neste contexto, o principal objetivo deste trabalho foi o de definir e implantar um método para controlar e gerenciar o acesso à estrutura de rede de computadores da PMPM-RS visando, por meio da Política de Segurança e critérios administrativos, criar perfis de controles para caracterizar formas de acesso a redes específicas, de acordo com as necessidades de cada usuário.

2. Estado da Arte

A partir dos trabalhos correlacionados estudados, elaborou-se um quadro destacando as principais características dos mesmos, comparando-os à solução apresentada neste artigo. Estas características são apresentadas no Quadro 1.

Quadro 1 – Estudo Comparativo

Trabalhos	***Software* e ferramentas utilizadas**	**Resultados alcançados em relação aos objetivos**
Trabalho 1 (PEIXOTO, 2004)		- colaborar como instrumento de compreensão didático-metodológico; no contexto das inúmeras vulnerabilidades técnicas e humanas inseridas nas Organizações, agregando-se a futura elaboração de uma ferramenta para melhor gerir a segurança das informações.
Trabalho 2 (MOLINA, SILVEIRA e SANTOS, 2015)	*Zabbix*, *Packet Tracer*, SARG	- Maior gerência e segurança da rede com as VLANs e DMZ - Com o *Zabbix* foi possível ter respostas muito mais rápidas e tomar decisões mais acertadas - Com um controle maior da rede é possível fazer uma maior previsão em quesitos como gerência e escalabilidade.
Trabalho 3 (NEVES, MACHADO e CENTENARO, 2014)	*Firewall PfSense*	- Filtragem de origem e destino IP, protocolo IP, portas de origem e destino para tráfegos de protocolos UDP e TCP; - Habilidade de limitar através de uma política de regras, conexões simultâneas; - Opção de realizar ou não os relatórios baseados somente em regras selecionadas; - Habilidade de criação de grupos de endereços, redes e portas visando à facilidade de gerenciamento e a clareza das regras criadas; - Capacidade de gerenciamento de tabela de estados; - Interface *web* de extrema facilidade de gerenciamento;
Solução Implementada	Autenticação por portal *(hotspot)*	- controle e gerência do acesso à estrutura de rede de computadores da Prefeitura Municipal de Palmeira das Missões – RS

Analisando-se os trabalhos estudados, verifica-se que existem problemas em comum, que necessitaram de melhorias na questão da segurança da informação. Os problemas destacados envolvem dificuldades de gerenciamento, desempenho e segurança, principalmente.

No quadro 1, pode-se visualizar os diferentes tipos de *software* e ferramentas que foram utilizados para solucionar os mais diversos problemas e os resultados obtidos em cada um dos trabalhos. Um fato interessante é que todos os trabalhos visam à questão de segurança da informação, tanto estudando conceitos e vulnerabilidades, quanto a aplicação de métodos em ambientes reais (organizações), permitindo que seus resultados pudessem ser comprovados. Sendo assim, pode-se constatar que, apesar de serem organizações diferentes, os problemas ligados às redes de computadores são comuns, principalmente quando se trata de segurança e gerenciamento de redes de computadores.

3. Solução Implementada

A solução implementada neste trabalho envolveu a definição e implementação de um método de autenticação para controle e gerenciamento da conexão dos usuários da rede de computadores da PMPM-RS para, assim, restringir e registrar os acessos conforme a Política de Segurança e contexto da segurança de rede baseada em perfil de usuários. A solução permitiu controlar o acesso dos usuários e diminuir o tráfego na rede, por meio de técnicas de autenticação usando o protocolo 802.1x, utilizando-se perfis de acesso e estabilidade definida por VLANs.

O método de pesquisa empregado neste trabalho foi o estudo de caso. Segundo Yin (2001), os estudos de caso são uma metodologia de pesquisa adequada quando se colocam questões do tipo "como" e "por que", que fazem parte do objetivo geral deste trabalho – como implantar um método de acesso a rede de computadores, por exemplo.

A aplicação do método de gerenciamento teve início a partir de agosto de 2016, com a criação de um servidor *web*. Esse servidor *web* é o responsável por armazenar e trocar informações com os computadores da rede. No caso do usuário, é usado um *browser*, como o *Google Chrome* ou o *Mozilla Firefox*. No lado do servidor, porém, existem várias opções de *softwares* disponíveis, mas todos têm uma tarefa semelhante: gerenciar a transferência de dados entre clientes e servidores via HTTP, o protocolo de comunicações da *web* (FIELDING; GETTYS, 1999).

O método escolhido para o controle e gerenciamento de acesso dos usuários foi o de autenticação por portal, denonimada "*hostpot*", que consiste em uma página "*web Landing".* Esta autenticação pode ser apresentada por um *"layer 3"* ou "*layer 2".* O *layer 2* apenas possui a capacidade de trabalhar com *MAC addresses*. Isso permite que ele se comunique apenas baseado em endereços *MAC;* ele também propaga todo *broadcast* e não tem capacidade de interligar redes ou sub-redes. O *layer 3*, além de código *MAC*, tem a capacidade de roteamento e também trabalha com endereçamento lógico. Dessa forma, tem a capacidade de identificar redes e sub-redes (endereço IP e máscara), possibilitando a interconexão de redes ou sub-redes, sendo utilizado para a criação de VLANs (CHEN, 2010).

Depois de ser redirecionado para uma página *web* que pode exibir autenticação, pagamento, políticas de uso aceitável ou outras credenciais válidas, o *host* do usuário concorda com as informações fornecidas. Logo após, é concedido ao usuário o acesso à Internet de forma condicional, isto é, restrito em alguns *sites*. Esses serviços de *hostpot* são usados cada vez mais para obter uma melhor segurança, tanto nas redes cabeadas

quanto nas não cabeadas, para acesso empresarial e residencial, por exemplo, em edifícios de apartamentos, quartos de hotel, centros de negócios, etc. (CHEN, 2010).

A página de *login* para acesso à Internet apresentada ao usuário é armazenada localmente no *gateway* ou no servidor de hospedagem na *web*. Isso requer acesso a uma lista aprovada de acesso, ou "*white-list*", uma característica essencial de uma empresa segura.

O hotspot requer o uso de um navegador *web*. Este é geralmente o primeiro passo para que os usuários comecem a navegar na Internet, mas, se o usuário usar um programa específico para leitura de *e-mails* antes de abrir o navegador, vai perceber que a conexão não está funcionando. O acesso só será liberado quando o navegador for aberto e a conexão for validada (SONDAG; FEHER, 2007).

3.1 Definição dos Perfis de Acesso

O acesso a *sites* seguros e de qualidade, com conteúdos relevantes e que realmente atendam aos interesses ligados às funções exercidas pelos usuários, é um problema a ser considerado, diante da amplitude e diversidade de *sites* existentes na Internet. Assim, neste trabalho, foram verificadas as necessidades dos usuários de acordo com as funções exercidas, para que os mesmos tenham acesso a informações externas e sistemas existentes para efetivação do seu trabalho. Pôde-se, assim, definir os principais critérios de avaliação dos *sites* em que os usuários poderão ter acessos: conteúdo, objetivos do *site*; abrangência, propósito e funcionalidade.

Para a realização deste trabalho criou-se, para cada setor e/ou departamento da PMPM, um perfil de acesso à Internet. Os perfis podem ser alterados pelos administradores do sistema. Em alguns casos específicos, o usuário poderá requisitar acesso diferenciado. Para isso terá que detalhar, por escrito, suas necessidades reais de acessos. Isso significa uma possibilidade de usuários, do mesmo setor, possuírem perfis diferentes.

3.2 Desenvolvimento das regras

A parte da aplicação desenvolvida neste trabalho, em que são criadas as regras iniciais de controle, foi escrita em linguagem *script* no SO, testando-se em um Sistema Operacional *Ubuntu Linux*. Como suporte para armazenar os dados, foi utilizado o SGDB (Sistema Gerenciador de Bancos de Dados) *MySQL*, além da criação da página de *login* utilizando-se a linguagem de programação PHP. Com a integração do PHP com o *shell*, pela função "shell_exec" (nativa do PHP), foi possível um gerenciamento dinâmico nas regras de *firewall*.

Atendendo às finalidades deste projeto, foi criado um arquivo que faz as alterações iniciais de regras do sistema, sendo executado na inicialização do SO, a fim de que, ao iniciar o sistema, sejam executadas as rotinas a seguir descritas: exclusão de todas as regras e *firewall* pré-existentes; ativação do roteamento no SO; redirecionamento do tráfego de todos os endereços IPs da rede para o sistema de autenticação; criação das politicas de controle de tráfego; verificação dos usuários que possivelmente estavam conectados e a reconexão deles (função usada para o caso de uma queda no sistema ou reinicialização do servidor).

3.3 Aplicação do Método de Gerenciamento

A implementação do *hotspot*, método escolhido para este trabalho, foi realizada utilizando-se um servidor RADIUS e a aplicação *CoovaChilli*. Esta aplicação é responsável por distribuir números IPs (serviço DHCP) e a página de autenticação aos utilizadores que se conectem via *Wireless* (sem fios) ao servidor. A partir da conexão, a aplicação utilizando o *freeRADIUS* encarrega-se do registro e verificação da autenticação.

O *freeRADIUS* é uma implementação de RADIUS modular, de alta performance e rica em opções e funcionalidades. Esta inclui servidor, cliente, bibliotecas de desenvolvimento e muitas outras utilidades. Pode ser instalada em sistemas *Linux* e *Machintosh* (HASSELL, 2002). O *CoovaChilli* é uma aplicação composta por um conjunto de regras de *IPTables* que faz o controle de acesso dos usuários por meio de uma página *web* de autenticação, além de realizar a distribuição de IPs (serviço DHCP). Mais informações sobre o *CoovaChilli* podem ser acessadas no *site* <http://coova.org/CoovaChilli>.

Para o funcionamento adequado das autenticações é necessária a instalação e configuração dos arquivos da aplicação *Haserl*, responsável por criar *scripts* utilizando *shell* ou *Lua script*. O *Haserl* é um pequeno programa que usa *shell* ou Lua *script* para criar *scripts* .CGI (*Common Gateway Interface*) em páginas *web*. Ele é destinado a ambientes onde os arquivos PHP podem ser muito grandes. É um complemento necessário para o funcionamento da autenticação do *CoovaChilli*, visto que é necessário suporte para visualização da página onde o usuário fará a autenticação. Mais informações sobre o *Haserl* podem ser encontradas no site <http://haserl.sourceforge.net/>.

4. Testes e Resultados

Utilizando os recursos do *software Zabbix* foi possível monitorar e visualizar os relatórios de consumo de rede na PMPM-RS (ZABBIX,2017). Com a ajuda do *Zabbix* pode-se ter uma ideia de consumo de Internet na PMPM-RS. Para exemplificar este consumo, a Figura 1 apresenta o consumo de rede no período compreendido entre 13/12/2016 e 02/04/2017.

Figura 1 – Gráfico com o consumo de rede entre 13/12/2016 e 02/04/2017
(Fonte: dos autores, 2017)

Como se pode observar, analisando o gráfico da Figura 1, o consumo de Internet variou constantemente, atingindo picos mais elevados de consumo de Internet. Para que se possa ter uma ideia dos resultados que poderão ser atingidos com a implantação do sistema de gerenciamento e controle de acesso à Internet aqui apresentado, definiu-se um setor hipotético com 4 computadores sendo eles denominados A,B,C, e D, sendo eles monitorados com o *Radius* e o *Zabbix*. Este método simulado foi proposto diante da falta

de tempo para realizar a implantação completa em todos os setores, pois seria necessária uma dedicação e cuidado extra, envolvendo todos os funcionários e departamentos dentro da PMPM-RS.

Os gráficos apresentados nas Figuras 2, 3, 4 e 5 foram construídos após as permissões dos usuários hipotéticos terem sido configuradas adicionando restrições e bloqueios em *sites* mais comuns e mais acessados tais como redes sociais (*Facebook*), *YouTube*, sites nocivos e com conteúdo considerado impróprio. O acesso a esses *sites* foi totalmente liberado em determinados momentos, para que se pudesse simular como o fluxo de rede aumentaria caso estes *sites* fossem liberados.

Tendo como base este setor hipotético, utilizando o sistema de controle de usuário nos computadores, a simulação mostra que o consumo de Internet na rede diminuiria de 30% a 50%. Por exemplo, na simulação do computador A (Figura 2), pode-se verificar que, em cerca de 1 hora o consumo de Internet dobrou quando o seu usuário estava sem utilizar o sistema de controle, podendo acessar quaisquer *sites* na Internet, podendo navegar em *sites* desnecessários e fazer *downloads* de conteúdos na rede. Com o controle de usuários também é possível monitorar e identificar usuários que, mesmo bloqueados, tentam acessar determinados *sites* indevidos com frequência, podendo assim geram advertências para este usuário.

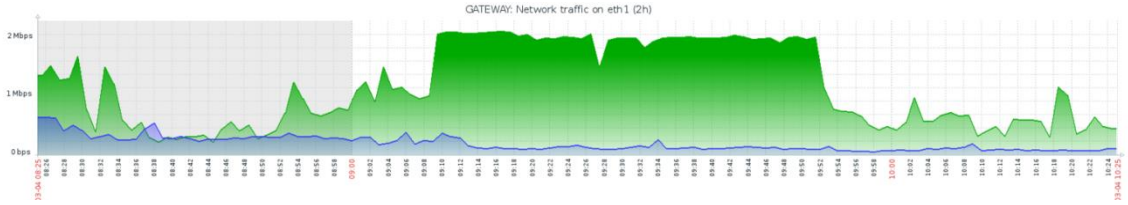

Figura 2 – Gráfico com o fluxo de rede no computador A (Fonte: dos autores, 2017)

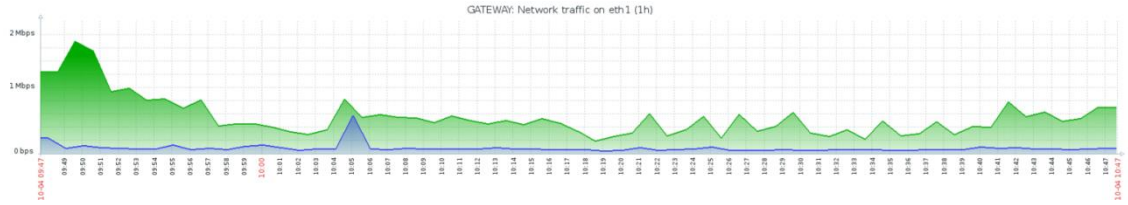

Figura 3 – Gráfico com o fluxo de rede no computador B (Fonte: dos autores, 2017)

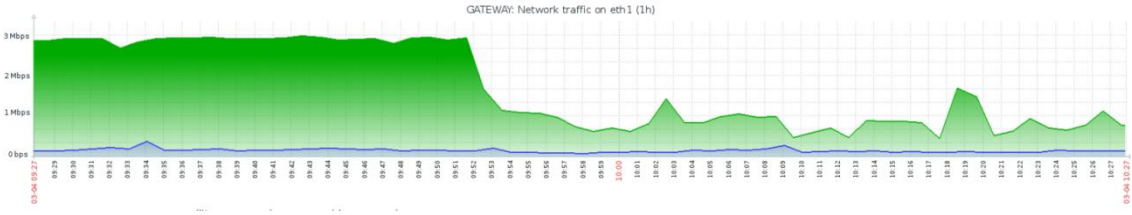

Figura 4 – Gráfico com o fluxo de rede no computador C (Fonte: dos autores, 2017)

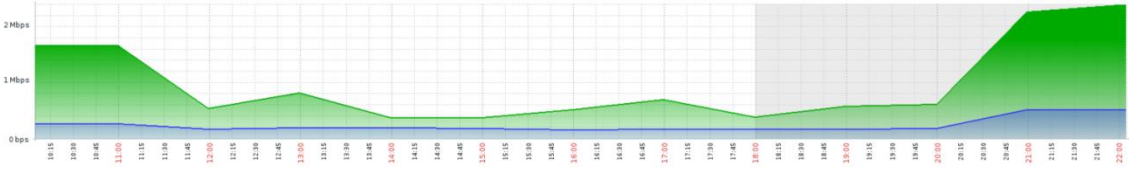

Figura 5 – Gráfico com o fluxo de rede no computador D (Fonte: dos autores, 2017)

Após todas as configurações e testes realizados, foi possível disponibilizar o *hotspot* totalmente gerenciado pelo RADIUS, trabalhando em conjunto com o

CoovaChilli. Com estes *softwares*, além do usuário ter muito mais segurança no seu acesso ele irá se relacionar com uma interface de autenticação amigável, fornecendo agilidade para o seu acesso. O usuário, ao se conectar ao ponto de acesso previamente conectado na interface eth1, receberá as configurações de IP automaticamente e a indicação do uso da página de autenticação para a liberação do acesso. O usuário ainda não estará permitido a navegar na Internet, sendo solicitado a inserir seu nome de usuário e senha no portal do *CoovaChilli*na página, como mostra a Figura 6.

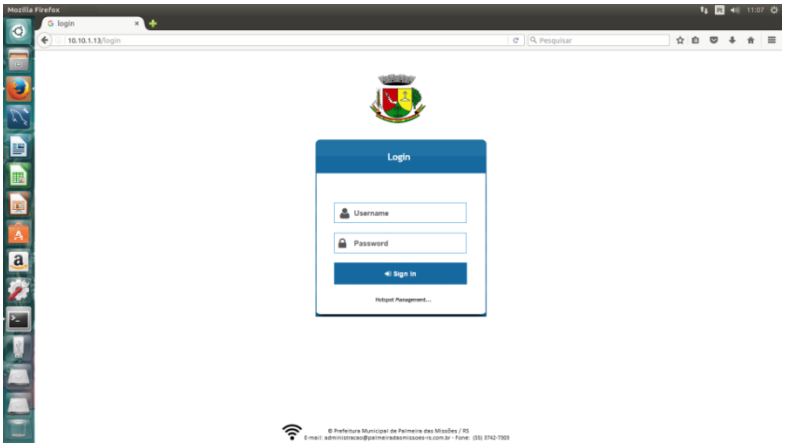

Figura 6 – Tela de **login** de usuário para acesso à Internet na PMPM-RS (Fonte: dos autores, 2017)

5. Considerações Finais

A implantação de um sistema para controlar e registrar o acesso dos usuários possibilita uma melhor segurança e controle dos acessos e, também, maior qualidade na questão de acesso à rede e na velocidade de tráfego, diminuindo principalmente a demanda de suporte no setor de informática da PMPM-RS, responsável pelo atendimento aos usuários.

Durante a realização desse trabalho notou-se que é necessário entender melhor como a organização funciona para compreender todas as necessidades dos funcionários em relação às informações que podem ou não ser acessadas via rede. Isso acaba tendo uma grande resistência dos funcionários, principalmente dos mais antigos que não compreendem muito bem como funcionará o controle de acesso à Internet.

Após a definição do método mais adequado de controle de acesso, realizou-se a simulação da aplicação do sistema de gerenciamento em um setor hipotético tendo em vista o controle de usuário com e sem o bloqueio de acesso a internet. A realização de testes ocorreu conforme a política de segurança da PMPM-RS, considerando o perfil e as necessidades de um determinado funcionário, visando ter melhor segurança e melhor qualidade no acesso à Internet.

O aplicativo de autenticação *FreeRadius* apresenta-se como uma opção adequada para implementação de controle de acesso à Internet, atingindo os objetivos específicos propostos, liberando o acesso só aos usuários autenticados, garantindo assim a segurança de banda de redes cabeadas e não cabeadas, ou simplesmente o controle dos usuários que devem utilizar deste recurso dentro da instituição.

Os resultados alcançados até o presente momento servem de base para uma ferramenta que possui abertura para agregar novas funcionalidades assim fornecendo uma solução adequada, não apenas para um mecanismo de segurança que possa autenticar um usuário, mas também é uma solução que pode informar quais os serviços disponíveis, qual o tamanho de consumo de banda por usuário, informando assim registros para possíveis auditorias.

Referências

CHEN, W. L. (2010) **A Proof of MITM Vulnerability in Public WLANs Guarded by Captive Portal**. Graduate Institute of Communication Engineering. Disponível em <http://journals.sfu.ca/apan/index.php/apan/article/view/80>. Acesso em 15 de junho de 2016.

FIELDING.; GETTYS.; (1999) **Hypertext Transfer Protocol -- HTTP/1.1** Disponível em: <https://www.rfc-editor.org/info/rfc2616> Acesso em 08 de novembro de 2016.

HASSELL, Jonathan et al. RADIUS. Editora O'Reilly, outubro. 2002.

MOLINA, D.; SILVEIRA S. R.; SANTOS, F. B. (2015) **Implantação de Um Ambiente de Segurança de Redes de Computadores:** um estudo de caso na Prefeitura Municipal de Palmeira das Missões – RS. Universidade Federal de Santa Maria (UFSM/CESNORS) – Frederico Westphalen – RS – Brasil. Trabalho de Graduação em Sistemas de Informação. Disponível em: <http://w3.ufsm.br/frederico/images/ImplantacaodeumAmbientedeSegurancadeRedesdeComputadoresUmEstudodeCasonaPrefeituradePalmeiradasMissoes.pdf> Acesso em 12 de Junho de 2016.

NEVES F. C.; MACHADO L. A.; CENTENARO R. F.; (2014) **Implantação de *Firewall PfSense.*** Universidade Tecnológica Federal do Paraná Departamento Acadêmico de Eletrônica - Curso Superior de Tecnologia em sistemas de Telecomunicações. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/3968/1/CT_COTEL_2014_2_02.pdf>. Acesso em 12 de Junho de 2016**.**

PEIXOTO, M. C. P. (2004) **Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas Organizações.** UNITRI – Centro Universitário do Triângulo Pró- Reitoria de Ensino de Graduação Curso de Ciência da Computação. Disponível em: <https: //e3baea88-a-62cb3a1a-s-sites.googlegroups.com/site/pedronunots/Home/academico-3/auditoria-de-seguranca-e-sistemas-de-informacao/artigos-relacionados/contexto_da_vulnerabil.pdf>. Acesso em 12 de Junho de 2016.

SONDAG, T.; FEHER, J. (2007) **Open Source Wifi Hotspot Implementation**. Information Technology and Libraries. Disponível em: <http://crawl.prod.proquest.com.s3.amazonaws.com/fpcache/14bb83ed7ff3950ef024f7c4996012c0.pdf > Acesso 15 de Junho de 2016.

YIN, R. K. (2001) **Estudo de Caso:** planejamento e métodos. 2. ed. Local: Bookman.

ZABBIX. (2017). **The Enterprise-class Monitoring Solution for Everyone**. Disponível em: < http://www.zabbix.com/download.php>. Acesso em: 04 de Abril de 2017.