Atividades de Laboratório 1

Apresentação:

As atividades de laboratório a seguir abordam as configurações básicas de monitoramento de dispositivos de uma rede utilizando o Zabbix. Essa abordagem irá permitir que os técnicos possam constatar na prática as informações apresentadas no curso, fazendo com que tenham contato com situações cotidianas envolvendo a gestão e o monitoramento de uma rede.

Neste laboratório será utilizado o ambiente de virtualização VirtualBox, onde será instanciada uma máquina virtual contendo um servidor Zabbix instalado. Nesta atividade, os usuários devem realizar acesso à aplicação Zabbix através do navegador de internet e realizar as configurações.

Cenário:

O cenário da aplicação que iremos montar está representado abaixo (Figura 1).

Neste cenário teremos uma máquina hospedeira que abrigará o servidor virtual contendo a instância do servidor Zabbix, responsável pelo monitoramento. Essa aplicação será acessada, via web browser, através da máquina hospedeira e serão realizadas configurações de monitoramento tendo como alvo a máquina virtual chamada *"Monitor1".*

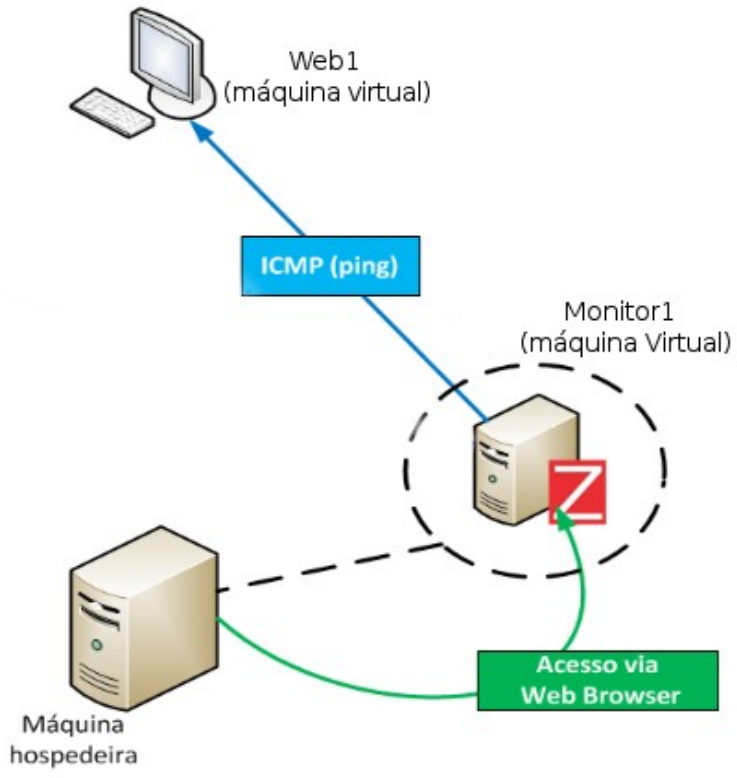

Figura 1: Cenário do laboratório

Etapa 1: Subir o ambiente virtual

A primeira etapa a ser realizada nesta atividade é subir a instancia da máquina virtual criada para hospedar o Zabbix. Nela estará rodando o servidor da aplicação onde todas as configurações serão realizadas. Para isso todos devem ir até o terminal de comandos e digitar: virtualbox

Outra opção seria clicar no atalho chamado “virtualbox” na àrea de trabalho

Após a execução do aplicativo deverá ser selecionada a máquina virtual *“Monitor1”* e apertar o botão “Iniciar”;

Pronto, já temos a máquina virtual no ar e rodando o servidor Zabbix;

Etapa 2: Acesso à aplicação

Uma vez que o servidor Zabbix esteja no ar, a próxima etapa é acessar a aplicação através de sua interface web e iniciar as configurações de monitoramento.

Para o primeiro acesso é necessário saber o endereço IP do servidor. Para isso é preciso realizar o login na máquina virtual e obter as informações. Para realizar o login utilizar as seguintes informações:

Usuario: wtr
Senha: wtr

Uma vez feito o login, obter o endereço ip do servidor através do seguinte comando:

/sbin/ifconfig

Uma vez de posse do endereço IP do servidor devemos agora ir até a máquina hospedeira, onde será realizado o acesso à interface web da aplicação.

Na máquina hospedeira acesse o browser e digite:

http://<endereco_ip_da_maquina_virtual>/zabbix

A tela de login da interface web do Zabbix será apresentada, como mostra a figura 2:

Figura 2: Tela de login do Zabbix

Para realizar o acesso, deve-se inserir as seguintes informações:
usuário: admin
senha: zabbix

Etapa 3: Configurando grupos e templates

Antes de partirmos para a adição de dispositivos a serem monitorados, devemos antes realizar algumas configurações que irão poupar muito trabalho quando for necessário configurar monitorar uma grande quantidade de máquinas.

No Zabbix, os dispositivos monitorados podem ser classificados em grupos, cada grupo apresentando uma série de configurações específicas que serão automaticamente aplicadas a todos os novos dispositivos associados àquele grupo.

Por essa razão, uma definição planejada dos grupos e das configurações pode economizar bastante tempo e recursos humanos à medida que a rede expande-se. Por essa razão, vamos iniciar esta etapa criando um novo grupo onde serão associados os dispositivos nas etapas seguintes. Para isso siga os passos:

3.1 Criando um novo Grupo:

3.1.1 Selecione a opção ***"Configuração"***;
3.1.2 No submenu exibido, selecione a opção ***"Grupo de Hosts"***;
3.1.3 Clique no botão ***"Criar Grupo de Hosts"***;
3.1.4 Defina ***"Servidores_Teste"*** como nome para o grupo de dispositivos;
3.1.5 Associar dispositivos anteriormente criados a "Servidores_Teste"(Opcional);
3.1.6 Clicar em ***"Salvar"***;

3.2 Criando um novo Template:

Após a criação de um novo grupo, a próxima etapa é criar um template contendo uma série de configurações específicas. Os templates podem ser posteriormente associados aos grupos.

3.2.1 Selecionar a opção ***"Configuração"***;
3.2.2 No submenu exibido, selecionar a opção ***"Template"***;
3.2.3 Clicar no botão ***"Criar Template"***;
3.2.4 Definir *"Template_Base"* como nome do novo template;
3.2.5 Clicar em ***"Salvar"***;

3.3 Criando uma Aplicação, Itens e Triggers:

Por si só, o template não representa alteração alguma a nenhum grupo associado a ele. As mudanças e customizações irão ocorrer através das configurações dos elementos que compõem o template: as aplicações, os itens e as triggers.

As aplicações são agrupamentos de itens que possuam características em comum. É comum encontrar aplicações como *“Disponibilidade”*, *“Sistema de Arquivos”*, *“Memória”*, *“Serviços”*, *“Rede”* e todas estas aplicações são compostas por itens dentro do escopo da descrição.

Os itens são informações específicas que são consultadas dos dispositivos monitorados. São exemplos de itens: *“Espaço livre no diretório /”*, *“Hora local de um dispositivo”*, *“Número de usuários conectados ao dispositivo”*.

As triggers são ações disparadas pelo zabbix quando algum dos itens atinge determinado valor de monitoramento pré-determinado. Através das triggers é possível, por exemplo, disparar um e-mail para o analista responsável quando a capacidade de CPU de um determinado roteador superar 90%.

O primeiro passo é criar uma aplicação onde seja possível configurar diversos itens e triggers para os itens.

3.3.1 Repetir as etapas 3.2.1 e 3.2.2;
3.3.2 Todos os templates serão exibidos em uma lista. Deve-se encontrar o template criado na etapa 3.2 (Template_Base). Na mesma linha deste template, do lado direito terá a indicação *“Aplicação(0)”* indicando que esse template ainda não possui nenhuma aplicação associada a ele.
3.3.3 Clicar em ***“Aplicações(0)”***;
3.3.4 Na nova tela que é exibida, no canto superior direito, clicar no botão *“Criar Aplicação”*;
3.3.5 Determinar *“Disponibilidade”* como nome da nova aplicação;
3.3.6 Clicar em ***“Salvar”***;

Criada a aplicação, aparecerá a lista de aplicações criadas contendo apenas a aplicação *“Disponibilidade”*. É possível observar, do lado direito, uma indicação *“Itens(0)”*, indicando que esta aplicação não possui nenhum item associado. Próximo passo é criar um item para esta aplicação. O item que será criado será um monitoramento de ping para que possa ser avaliada a disponibilidade do host:

3.3.8 Clicar em ***“Itens(0)”***;
3.3.9 Na nova tela que é exibida, no canto superior direito, clicar no botão ***“Criar Item”***;
3.3.10 Em ***“Nome”*** inserir *“Ping”*;
3.3.11 Em ***“Tipo”*** selecionar a opção *“Monitoração Simples”*;
3.3.12 Em ***“Chave”*** selecionar a opção *“icmpping[<ip>, <count>,<interval>,<size>,<timeout>]”*. Essa opção de monitoramento ping já vem pré-deteminada na base do Zabbix. Contudo o formado dos parâmetros não precisam ser seguidos à risca, podendo ser customizados. Deve-se apagar todos os parâmetros deixando apenas *“icmpping”*;
3.3.13 Em ***“Mostrar Valor”*** selecionar a opção *“Service state”*;
3.3.14 Em ***“Aplicações”*** selecionar a opção da aplicação criada

anteriormente (*“Disponibilidade”*);

3.3.15 Clicar em ***“Salvar”***;

Pronto. Até o momento já existe um grupo *“Servidores_Teste”* e este possui o template *“Template_Base”* associado. Já o template possui uma aplicação *“Disponibilidade”* e associado a esta aplicação existe um item *“Ping”* que é responsável por receber pacotes ICMP que serão utilizados para avaliar a disponibilidade dos dispositivos.

Após a criaçao do item *“Ping”* a lista exibindo o único item criado é apresentada. Nela é possível observar um link indicando *“Triggers(0)”*. Da mesma forma como os outros, indica que não existe qualquer trigger associada a este item. Precisamos agora criar ações que o zabbix deverá tomar sempre que parar de receber pacotes ICMP de determinado dispositivo.:

3.3.17 Na barra superior, selecionar a opção *“Triggers”*;

3.3.18 Clicar em ***“Criar Trigger”***;

3.3.19 Em ***“Nome”*** defirnir a frase: *“Host {HOSTNAME} indisponivel”*. A expressão *“{HOSTNAME}”* será substituida pelo nome do host que está sendo monitorado. Por exemplo, se o servidor *“Servidor VPN”* estiver sendo monitorado por esta trigger e, por alguma razão, este ficar indisponível será exibida a mensagem ***“Host Servidor VPN indisponível”***;

3.3.20 Em ***“Expressão”*** clicar em *“Adicionar”*;

3.3.21 Na janela *“Condição”* exibida:

3.3.21.1. Em ***“Item”*** clicar em selecionar;

3.3.21.2. Em ***“Grupo”*** selecionar “*Servidores_teste*” e em ***“Host”*** selecionar *“Template_Base”*. Será exibida lista de itens associados ao template. Selecionar *“Ping”*;

3.3.21.3. Em ***“Função”*** selecionar a opção *“Média do valor de um periodo T é = N”*.

3.3.21.4. Em ***“Última de (T)”*** indicar *“300”* segundos;

3.3.21.5. Em ***“N”*** indicar 0;

3.3.21.6. Clicar em ***“Inserir”***;

Essa expressão acaba de definir que se a média de recebimento de resposta dos pacotes ICMP (Ping) enviados nos últimos 300 segundos for igual a 0, ou seja, se o Zabbix não receber nenhuma resposta ping nos últimos 5 minutos, ele deverá agir.

3.3.22 Em ***“Severidade”*** indicar o valor *“Alto”;*

3.3.23 Clicar em ***“Salvar"***;

3.4 Criando Hosts de monitoramento:

Uma vez que já foi definido um template básico para todo dispositivo onde se pretenda apenas monitorar a disponibilidade, resta a tarefa de criar justamente o host a ser monitorado. Para isso deve-se executar a lista de ações:

3.4.1 No menu principal, clicar em ***“Configuração”***;

3.4.2 No submenu, clicar em ***“hosts”***;

3.4.3 No canto superior direito, clicar no botão ***"Criar host"***;
3.4.4 Em ***"Nome"*** indicar *"Web1"*;
3.4.5 Em ***"Grupos"*** remover qualquer grupo e selecionar apenas o grupo *"Servidores_Teste"*;
3.4.6 Em ***"Endereço IP"*** inserir o endereço IP da máquina virtual cliente, fornecido por este em sala (10.0.0.2);
3.4.7 Nas abas superiores, na sessão *"templates"* é possível notar que não há nenhum template associado ao host. Clicar em ***"Selecionar"***;
3.4.8 O grupo *"Template"* já deverá estar selecionado. Caso não esteja, em ***"Grupo"*** selecione *"Template"*. Na lista exibida, selecione o template criado nas etapas anteriores (*"Template_Base*"). Clicar no botão ***"Selecionar"***, no final da lista;
3.4.9 Clicar no botão ***"Adicionar"***;
3.4.10 Clicar no botão ***"Salvar"***;

Ao final será exibido dois hosts, "*Zabbix server"* e *"Web1"*, sendo que o *"Web1"* está utilizando as configurações de aplicação, itens e triggers herdadas de *" Template_Base"*.

3.5 Produzindo mapa de monitoramento:

Após a criação dos hosts que serão monitorados, vamos adicionar referências a estes dispositivos a um mapa de visualização.

A produção de mapas de visualização é uma funcionalidade bastante interessante do Zabbix, permitindo aos analistas organizarem visualmente todos os dispositivos monitorados em sua instituição. Um mapa bem organizado, permite uma gestão eficiente e respostas imediatas aos incidentes alertados pelo Zabbix.

O objetivo aqui é adicionar os dois hosts criados ao mapa. Para isso seguem as indicações a serem realizadas:

3.5.1 No menu principal, clicar em ***"Configuração"***;
3.5.2 No submenu exibido, clicar em ***"Mapas"***;
3.5.3 Clicar no mapa listado (***"Mapa da instituição"***);
3.5.4 Após abrir o mapa em sua versão de edição, deve-se clicar no botão **"+"** ao lado da palavra "Ícone";
3.5.5 Um ícone será exibido no site. Você poderá movê-lo para qualquer lugar do site, basta para isso clicar sobre o ícone e arrastá-lo.
3.5.6 Dê um duplo clique no ícone para editarmos algumas informações:

3.5.6.1. Em ***"Tipo"*** selecione a opção "host";
3.5.6.2. Em ***"Texto"*** insira o nome do host *"WEB"*;
3.5.6.2. Em ***"Host"*** clique no botão "Selecionar";
3.5.6.3. Na janela que é exibida, em grupos, escolha

“Servidores_Teste”;

3.5.6.4. Na lista exibida escolha “Web1”;

3.5.6.5. Em ***“Ícone (padrão)”***, selecionar “Server_(96)”;

3.5.6.6. Clicar no botão ***“Aplicar”***;

3.5.6.7. Clicar no botão ***“Fechar”***;

3.5.7 No canto superior direito, clicar em ***“Salvar”*** para salvar as alterações realizadas no mapa;

Para a visualização do mapa configurado clique, no menu principal em ***“Monitoramento”*** e, no submenu em ***“Mapa”***. Com isso é possível realizar o monitoramento em tempo real dos dois dispositivos configurados. Se houver um circulo vermelho em volta do *“Web1”* isso indica que o servidor está indisponível. Você como responsável pelo servidor deve identificar o problema. *DICA: veja se a máquina virtual está rodando :D!!!*

Reflexão:

Tão importante quanto ter as habilidades e conhecimentos necessários para configurar e lidar com os problemas que possam vir a surgir em uma rede é ter um bom monitamento, parte fundamental para uma boa gestão de rede. Os eventos e incidentes que ocorram no ambiente de qualquer instituição deve ser prontamente tratado, não havendo espaço para intervalos onde o problema ainda não havia sido sequer notado.

Existem diversas ferramentas de monitoramento, cabe aos analistas avaliarem e implantarem aquela que melhor adeque-se ao seu ambiente em particular e às políticas da empresa.

Atividades de Laboratório 2

Apresentação:
As atividades de laboratório a seguir abordam as configurações básicas de monitoramento de dispositivos de uma rede utilizando o Cacti. As diversas etapas das atividades irão possibilitar a familiarização com o ambiente da ferramenta e com o monitoramento de dispositivos através desta.

Neste laboratório também será utilizado o ambiente de virtualização *VirtualBox*, onde será instanciada uma máquina virtual contendo um servidor Cacti instalado. Nesta atividade, os usuários devem realizar acesso à aplicação Cacti através do navegador de internet e realizar as configurações.

Cenário:
O cenário da aplicação que iremos montar está representado abaixo (Figura 3).

Neste cenário teremos uma máquina hospedeira que abrigará o servidor virtual contendo a instância do servidor Cacti, responsável pelo monitoramento. Essa aplicação será acessada, via web browser, através da máquina hospedeira e serão realizadas configurações de monitoramento tendo como alvo as máquinas do instrutor e monitor deste mini-curso.

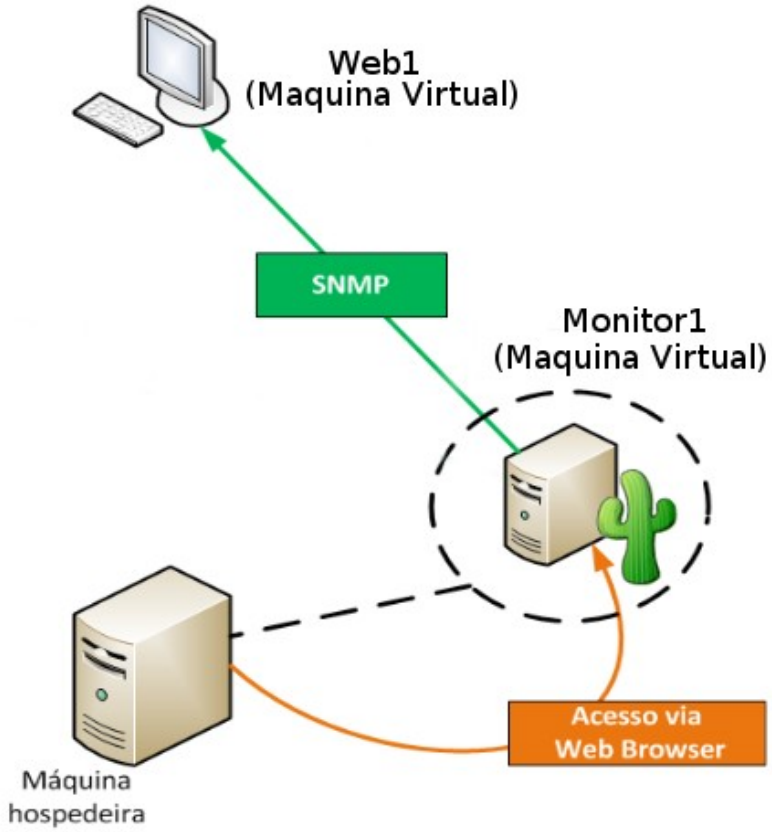

Figura 3: Cenário do laboratório

Etapa 1: Subir o ambiente virtual

A primeira etapa a ser realizada nesta atividade é subir a instancia da máquina virtual criada para hospedar o Cacti. Nela estará rodando o servidor da aplicação onde todas as configurações serão realizadas.

Para isso todos devem ir até o terminal de comandos e digitar:

virtualbox

Após a execução do aplicativo deverá ser selecionada a máquina virtual "*Monitor1*" e apertar o botão "Iniciar";

Pronto, já temos a máquina virtual no ar e rodando o servidor Cacti;

Etapa 2: Acesso à aplicação

Uma vez que o servidor Cacti esteja no ar, a próxima etapa é acessar a aplicação através de sua interface web e iniciar as configurações de monitoramento.

Para o primeiro acesso é necessário saber o endereço IP do servidor. Para isso é preciso realizar o login na máquina virtual e obter as informações. Para realizar o login utilizar as seguintes informações:

Usuario: wtr
Senha: wtr

Uma vez feito o login, obter o endereço ip do servidor através do seguinte comando:

/sbin/ifconfig

Uma vez de posse do endereço IP do servidor devemos agora ir até a máquina hospedeira, onde será realizado o acesso à interface web da aplicação.

Na máquina hospedeira acesse o browser e digite:

http://<endereco_ip_da_maquina_virtual>/cacti

A tela de login da interface web do Cacti será apresentada, como mostra a figura 4:

Figura 4: Tela de login do cacti

Para realizar o acesso, deve-se inserir as seguintes informações:
usuário: Admin
senha: admin

Etapa 3:

3.1 Adicionando novo Dispositivo:

O primeiro passo para o monitoramento através do Cacti é justamente a adição de um novo dispositivo na ferramenta. Para isso será necessário preencher o cadastro com informações específicas de cada novo dispositivo a ser monitorado. Vejamos a seguir as ações necessárias:

3.1.1 Clicar em ***"Console"***;
3.1.2 No submenu "Management"clicar em ***"Devices"***;
3.1.3 No canto superior direito, clicar em ***"Add"***;
3.1.4 Em ***"Description"*** preencher "WEB";
3.1.5 Em ***"Hostname"*** preencher com o endereço IP da máquina virtual *"Cliente"* (10.0.0.2);
3.1.6 Em ***"Host Template"*** selecionar "Generic SNMP-enabled Host";
3.1.7 Em ***"SNMP Version"*** selecionar "Version 2";
3.1.8 Em ***"SNMP Community"*** preencher "wtrcom";
3.1.9 Clicar em ***"Create"***;

Após a adição do novo dispositivo já será possível visualizar, na parte superior da tela, algumas informações de sistema coletadas (Hostname, Location, Contact, etc).

3.2 Criando gráficos para o novo Dispositivo:

Uma vez que os dois dispositivos foram adicionados ao monitoramento é preciso definir quais informações serão obtidas deles. Para isso é preciso criar gráficos de monitoramento para cada um deles.

Os gráficos não precisam ser definidos de forma igual para os dispositivos. Você pode customizar os gráficos de acordo com o seu interesse. Por exemplo, você pode querer monitorar a quantidade de dados trafegados para um determinado servidor e a quantidade de erros de entrada e saída em outro servidor.

3.2.1 Clicar em ***"Devices"***;
3.2.2 Na lista de dispositivos exibida, clicar em *"WEB"*;
3.2.3 No canto superior direito, clicar em ***"Create Graphs for this Host"***;
3.2.4 Marcar a checkbox na linha onde a *"Description"* do item esteja indicando ***"eth0"***;
3.2.5 Clicar em ***"Create"***;

3.2.6 Em ***"Select a graph type"*** selecionar a opção *"In/Out Erros/Discarded Packets"*;
3.2.7 Novamente marcar a checkbox na linha onde a *"Description"* do item esteja indicando ***"eth0"***;
3.2.8 Clicar em ***"Create"***;

3.3 Organizando árvores de gráficos

Criados diversos gráficos para os dispositivos, é necessário organizá-los para facilitar a visualização. O Cacti possui uma opção de organizar todos os gráficos em Árvores de gráficos. A seguir as ações necessárias para criar essas estruturas e organizar o seu monitoramento:

3.3.1 Clicar em ***"Console"***;
3.3.2 No submenu ***"Management"***, clicar em *"Graph Tree"*;
3.3.3 No canto superior direito, clicar em ***"Add"***;
3.3.4 Em ***"Name"*** definir *"Monitoramento WEB"*;
3.3.5 Em ***"Sorting Type"*** selecionar a opção *"Alphabetic Ordering"*;
3.3.6 Clicar em ***"create"***;

Nesse momento já está criada a árvore de gráfico. Resta agora associar os gráficos dos dispositivos criados à árvore.

3.3.7 No canto superior direito, clicar em ***"Add"***;
3.3.8 Em ***"Tree item Type"***, selecionar a opção *"Graph"*;
3.3.9 Em ***"Graph"***, selecionar a opção *"WEB – Traffic – eth0"*;
3.3.10 Em ***"Round Robin Archive"*** selecionar a opção *"Daily (5 Minutes Average)"*;
3.3.11 Clicar em ***"Create"***;

3.3.12 Repetir as etapas 3.2.7 a 3.2.11 para todos os gráficos iniciados com "WEB - *", apresentados na lista em "Graph" (etapa 3.2.9);

3.3.13 Clicar em "Save";
3.3.14 Repetir as etapas 3.2.7 a 3.2.13 agora para o dispositivo "PC do Instrutor";

3.4 Visualizando gráficos

Gráficos criados e organizados em árvores, resta a principal tarefa. Analisar os gráficos que estão sendo gerados em tempo real:

3.4.1 No menu principal, clicar em "Graph", ao lado de "Console";
3.4.2 No canto esquerdo, clicar na árvore "Monitoramento WEB";
3.4.3 Analisar cada um dos gráficos produzidos pelo monitoranento;

3.5 Configuração do Weathermaps

Weathermaps é um plugin *"open source"* de visualização de rede que ler os dados via RRDtool e mostra o resumo da atividade da rede. Ao clicar na aba *"weathermap"* ao lado de *"graphs", teremos um map vazio. O objetivo será monitorar os dois servidores virtuais. Para isso, execute as seguintes ações:*

3.5.1 No menu principal, clicar em ***"Console"***;
3.5.2 No canto esquerdo, clicar em ***"Weathermaps"***;
3.5.3 Na janela do Weathermaps, clicar ***"servidores.conf"*** ;
3.5.4 Nesse momento, estamos na página de edição. Clicar em ***"Add Node"****, irá aparecer uma "+" no cursor do mapa. Então basta clicar na tela para adicionar o host no local desejado;*
3.5.5 Clicar no icone criado;
3.5.6 Na janela *"Node Properties"*, em ***"Label"*** preencher com "Monitor1";
3.5.7 Em *"Icon Filename",* selecione ***"images/Host.png"***
3.5.8 Clicar em ***"Submit";***
3.5.9 Repita os passos 3.5.4, 3.5.5, 3.5.6, 3.5.7 e 3.5.8 para o host *"Web1";*
3.5.10 Clicar em ***"Add Link",*** em seguinda clique em *"Monitor1"* e *"Web1"*. Irá aparecer um link entre os dois servidores;
3.5.11 Clicar no link entre os dois servidores;
3.5.12 Na janela *"Link Properties",* Em *"Data Source"* clicar em ***"[Pick from Cacti]"****;*
3.5.13 Na janela *"Pick a data source", Em* ***"Host"*** *selecione "Web1";*
3.5.14 Clicar em ***"Web1 – Traffic – 10.0.0.2 – eth0"***;
3.5.15 Clicar em ***"Submit";***
3.5.15 Por fim, clicar em ***"Return to cacti";***

Agora, ao clicar na aba "weathermap" ao lado de "graphs", teremos o tráfego entre os dois servidores.

Reflexão:
O monitoramento da rede não resume-se à atividade de acompanhamento em tempo real do estado dos dispositivos de uma instituição. O monitoramento vai além. Dentro da tarefa de monitorar a rede de uma institutição é importante a coleta e dados para uma análise gerencial e estratégica da saúde da rede e para o levantamento das necessidade a curto, médio e longo prazos.

O Cacti traz essa possibilidade ao analista, produzindo gráficos que irão apresentar de maneira clara e eficiente os dados coletados e possibilitando a geração de relatórios técnicos que fundamentarão as decisões.

Atividades de Laboratório 3

Apresentação:
As atividades de laboratório a seguir abordam as configurações básicas de gerencia de endereços IPs de uma rede utilizando o PHPIPAM. As diversas etapas das atividades irão possibilitar a familiarização com o ambiente da ferramenta e com a gerencia dos endereços IPs através desta.

Neste laboratório será utilizado o mesmo ambiente de virtualização anterior, onde temos a máquina virtual contendo o servidor Zabbix e Cacti instalado. Nesta atividade, os usuários devem realizar acesso à aplicação PHPIPAM através do navegador de internet e realizar as configurações.

Etapa 2: Acesso à aplicação

Uma vez de posse do endereço IP do servidor devemos agora ir até a máquina hospedeira, onde será realizado o acesso à interface web da aplicação.

Na máquina hospedeira acesse o browser e digite:

http://<endereco_ip_da_maquina_virtual>/phpipam

A tela de login da interface web do phpipam será apresentada, como mostra a figura 5:

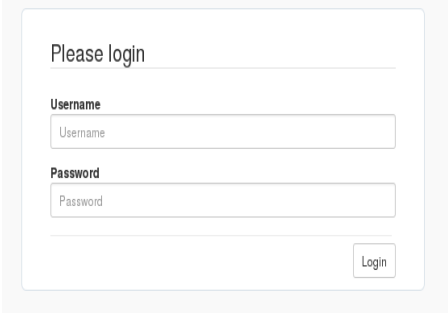

Figura 5: Tela de login do phpipam

Para realizar o acesso, deve-se inserir as seguintes informações:
usuário: Admin
senha: wtr

Etapa 3: Configurando hieraquia de rede

Antes de partirmos para a adição de endereços IPs a serem gerenciados, devemos antes planejar a hieraquia da rede. Dessa forma, poupa-se muito trabalho quando for necessário inserir uma grande quantidade de endereços.

No PHPIPAM, os endereços podem ser armazenados em pasta e subpastas (hieraquia de arvores), conforme a figura 6:

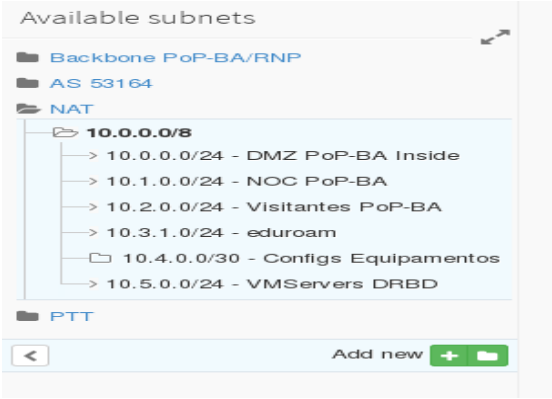

Figura 6: Tela de login do phpipam

Por essa razão, uma definição planejada da hieraquia da rede pode economizar bastante tempo e recursos humanos à medida que a rede expande-se. Por essa razão, vamos iniciar esta etapa criando uma pasta para nosso cenário onde serão associados os dispositivos nas etapas seguintes. Para isso siga os passos:

3.1 Criando um nova Pasta:

3.1 Adicionando nova Pasta:

O primeiro passo para o gerenciamento através do PHPIPAM é justamente a criação da hieraquia de rede na ferramenta. Para isso será necessário escolher entre IPv4 ou IPv6 (Esse menu IPv4 e IPv6 podem ser editados, além de inserir mais abas também. Por exemplo: VLAN). Vejamos a seguir as ações necessárias:

3.1.1 Clicar em ***"IPv4"***;
3.1.2 No submenu "Available subnets" clicar no simbolo de uma pasta;
3.1.3 Na janela nova, em ***"Name"*** preencher "NAT" e clique em *"Add"*;
3.1.4 No submenu *"Available subnets"* clicar em ***"+"*** *em Add new;*
3.1.5 Na janela nova, em ***"Subnet"*** preencher com *"10.0.0.0/8"*;
3.1.6 Em ***"Description"*** preencher com *"Rede Interna"*;
3.1.7 Em ***"Master Subnet"*** selecione a pasta que criamos anteriomente "*NAT"*;
3.1.8 Clicar em ***"Add"***;
3.1.9 No submenu *"Available subnets"* clicar em ***"+"*** *em Add new;*
3.1.10 Na janela nova, em ***"Subnet"*** preencher com *"10.0.0.0/24"*;
3.1.11 Em ***"Description"*** preencher com *"Servers DMZ"*;
3.1.12 Em ***"VLAN"*** selecione "4001 (Servers DMZ)";
3.1.13 Em ***"Master Subnet"*** selecione a *"Rede interna"*;
3.1.14 Clicar em ***"Add"***;

Após organizar a hieraquia da Rede Interna já será possível inserir os servidores na rede DMZ. Até esse ponto, estaremos dentro da subrede *"Server DMZ".* Caso contrario, no submenu *"Available subnets" clique na subrede* "10.0.0.0/24". Agora vamos inserir os servidores, na parte inferior da janela em

“Visual subnet display” faça as ações abaixo:

3.2 Adicionando endereço IP

3.2.1 Clicar no primeiro endereço, quandro com ***“.1”***;
3.2.2 Na janela nova, em ***“Hostname”*** preencher “Monitor1”;
3.2.3 Em ***“Description”*** preencher com *“Servidor de monitoramento”*;
3.2.4 Clicar em ***“Add IP”***;
3.2.5 Adicione o servidor *“web1”* repetindo 3.2.1 com o endereço “.2”, 3.2.2 com o “Hostname” “Web1” e 3.2.3 com a descrição “Servidor de aplicação” e 3.2.4

Reflexão:
O PHPIPAM é um software livre, bastante customizável, que permite gerencia de endereços IPv4 e IPv6 de maneira muito eficaz, permitindo por exemplo, configurações de blocos e em seguida, solicitar a ferramenta um scan sobre aquele bloco, registrando o resultado dos IPs em uso com a descrição opcional, baseado no reverso do DNS. Ainda, permite a gerencia de VLANs em uso, associando-as aos blocos cadastrados. Com esta ferramenta, o analista irá documentar e organizar sua rede maneira clara e eficiente.