

Sessão técnica: Usando Zabbix para Monitoramento

Data: 17/10/2019

Hora: 14h às 18h

Local: IFSertão-PE Campus Petrolina / Lab. CUBO

Instrutor: Cleiton Rodrigues de Souza

CV instrutor: <http://lattes.cnpq.br/3801524431020830>

Site: <https://crs.eti.br>

Laboratórios para prática com Zabbix



Instruções para a realização do laboratório com Zabbix.

A Empresa TreinaTI oferece cursos de capacitação na área de TI.

Em seu prédio possui dois laboratórios de informática contendo, cada um, 10 computadores. Além disso possui uma área administrativa contendo o setor de RH e Diretoria, o setor Financeiro, a coordenação dos cursos e o setor de TI.

A empresa possui cobertura WiFi nos ambientes e também possui um servidor Web hospedando o site da empresa e o ambiente virtual de aprendizagem (Moodle). Também possui um firewall na rede interna que compartilha o acesso à internet.

A diretoria, após reclamação dos usuários acerca de problemas durante as aulas referente ao acesso à internet, solicitou ao setor de TI que tomasse providências quanto a resolução do problema. Além das reclamações referente à internet, também relataram que, por vezes, a rede WiFi fica inacessível. Outro problema estava relacionado à disponibilidade do sistema Moodle utilizado pelos professores e alunos para as aulas.

Diante disso, o chefe de TI contratou **VOCÊ** para implantar um servidor de monitoramento. Ele verificou que os problemas de inacessibilidade da rede WiFi e acesso nos laboratórios se devia ao fato de que, ao sair dos ambientes, os professores e colaboradores desligavam a energia de toda a sala, conseqüentemente desligando *switchs* e *access points*, tornando o acesso indisponível. Ao retornar, não religavam toda a energia, ficando alguns equipamentos desligados. Quanto ao Moodle, ele observou que em dados momentos o sistema ficava travado devido a falta de recursos de *hardware* no servidor. Portanto, com a solução de monitoramento que **VOCÊ** vai implementar, o chefe de TI poderá, com antecedência, verificar a indisponibilidade dos equipamentos de rede como *switchs* e APs, além de monitorar a disponibilidade do portal Moodle e do serviço *web apache2*.

A imagem a seguir demonstra a situação atual da empresa e sua configuração de rede.

SERVIDORES
 pfSense: 192.168.1.1/24
 ZabbixSRV: 192.168.1.2/24
 WebSRV: 192.168.1.3/24

SWITCHS
 SWDIST01: 192.168.1.11/24
 SWADM01: 192.168.1.12/24
 SWLABI01: 192.168.1.13/24
 SWLABI02: 192.168.1.14/24

ACCESS POINTS
 APADM01: 192.168.1.15/24
 APLAB01: 192.168.1.16/24
 APLAB02: 192.168.1.17/24

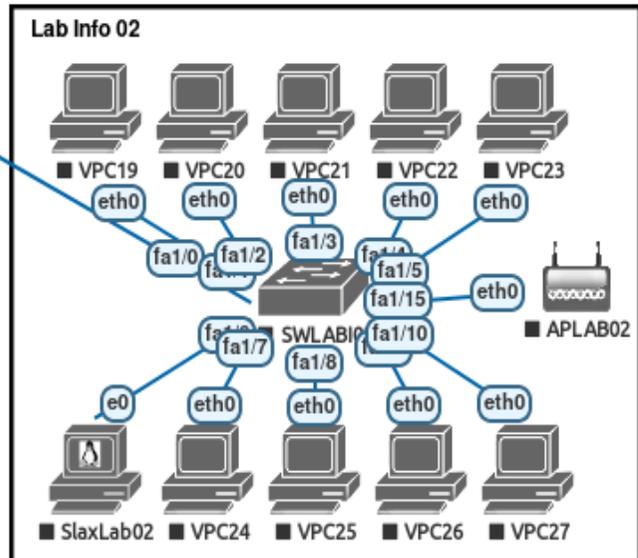
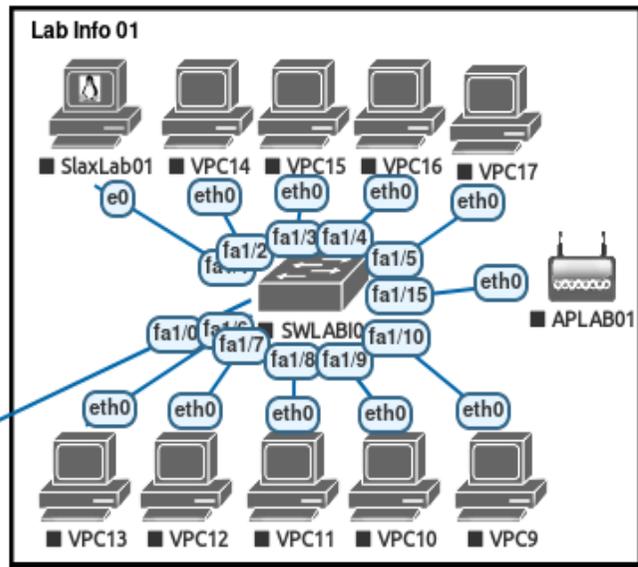
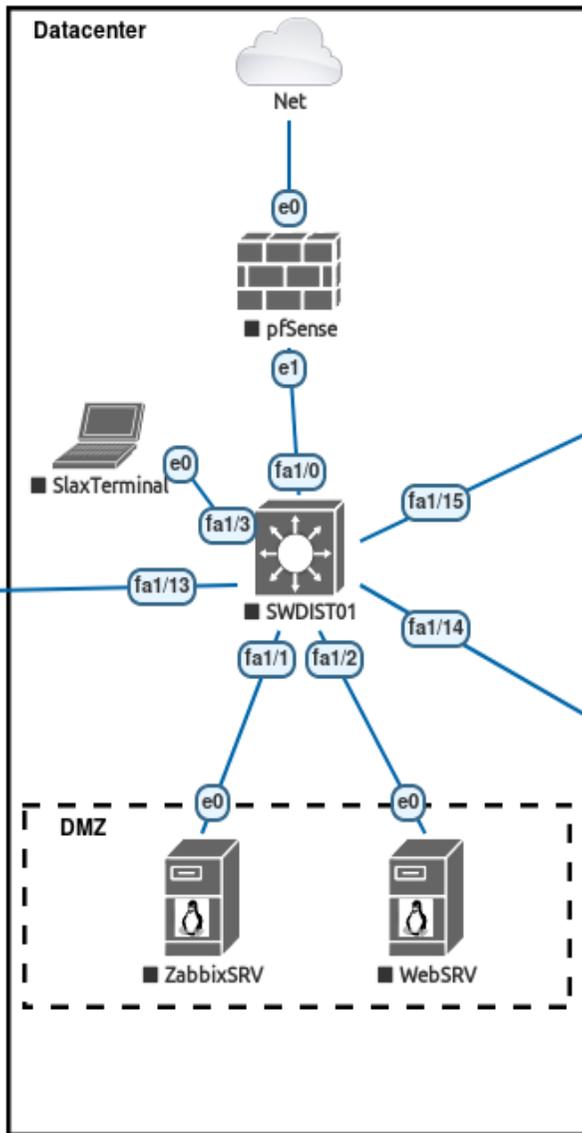
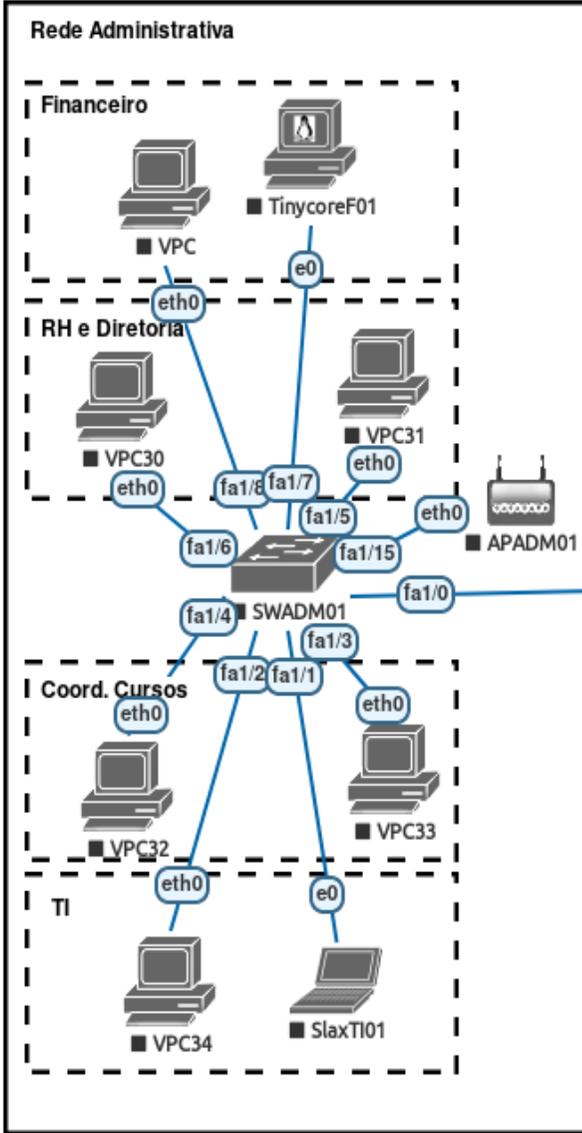
SISTEMAS
 www.treinati.com.br
 moodle.treinati.com.br
 zabbix.treinati.com.br

USERS | SENHAS
 pfSense
 admin | qwe123

ZabbixSRV
 root | qwe123

Frontend Zabbix
 Admin | zabbix

WebSRV
 root | qwe123



O servidor Zabbix já encontra-se pré-instalado, basta apenas configurar os hosts e serviços a serem monitorados. Nesse laboratório vamos:

1. Monitorar todos os hosts com monitoração simples por ICMP;
2. Monitorar os servidores com Zabbix Agent;
3. Monitorar o serviço HTTP e HTTPS do servidor web;
4. Monitorar os portais de serviço (Site e Moodle) da empresa.

OBS.:

- Não abra outros aplicativos, utilize apenas o necessário para evitar travamento do computador!
- Por ser um ambiente virtualizado em hardware de baixo poder de processamento, alguns cenários poderão não demorar tempo até obter respostas!

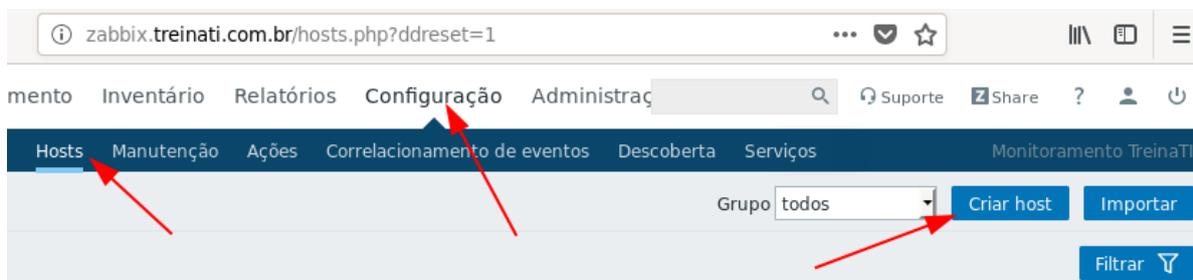
No seu computador, abra o software VirtualBox, expanda a sessão LabZabbix, selecione todas as máquinas virtuais (VMs) e inicie-as. Aguarde a inicialização!

Identifique a janela da VM **Debian10-XFCE**, use o login **user** e senha **qwe123**.

Se tudo correr bem, a partir de agora você utilizará a VM **Debian10-XFCE** para realizar todas as configurações. Todos os trabalhos a partir de agora serão através dessa VM.

1. Monitorar todos os hosts com monitoração simples por ICMP:

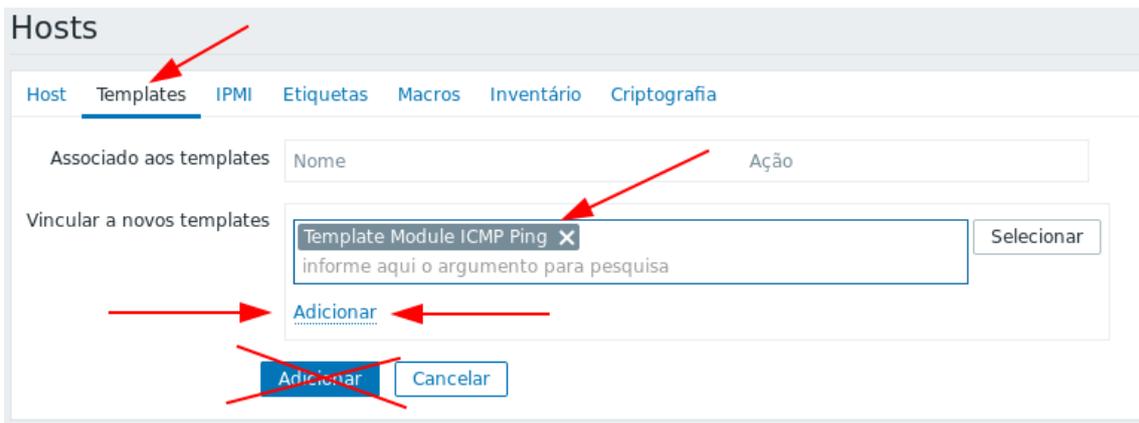
1. Abra o navegador Firefox;
2. Acesse o endereço: <http://zabbix.treinati.com.br> ;
3. Faça login com usuário **Admin** e senha **zabbix**;
4. Acesse os menus: Configuração > Hosts;
5. Clique no botão “Criar Host”;



6. Vamos cadastrar o servidor **WebSRV** (vide cenário). Preencha os campos como a seguir, o que não constar deixe como está:

- Seção Host:
- Nome do host: webserv
- Nome visível: webserv
- Grupos: Linux servers (basta digitar para aparecer...)
- Interfaces do agente: 192.168.1.3

- Seção Templates:
- Vincular a novos templates: digite **icmp** para pesquisar, escolha a opção Template Module ICMP Ping;
- **CUIDADO**: clique no link “Adicionar” não clique no botão “Adicionar” ainda!



- Após vincular o template ICMP no passo anterior, clique no botão “Adicionar”;



- Após adicionar, o host aparecerá na lista como abaixo:

<input type="checkbox"/>	Nome ▲	Aplicações	Itens	Triggers	Gráficos	Descoberta	Web	Interface	Templates	Status	Disponibilidade	Criptografia do
<input type="checkbox"/>	websrv	Aplicações 1	Itens 3	Triggers 3	Gráficos	Descoberta	Web	192.168.1.3: 10050	Template Module ICMP Ping	Ativo	ZBX SNMP JMX IPMI	NENHUM

7. Agora refaça os passo 5 e 6 para cadastrar o servidor **pfSense**, lembre-se de alterar as seguintes informações:

- Seção Host:
- Nome do host: **pfSense**
- Nome visível: **pfSense**
- Grupos: Linux servers (basta digitar para aparecer...)
- Interfaces do agente: **192.168.1.1**
- Seção Templates:

- Vincular a novos templates: digite icmp para pesquisar, escolha a opção Template Module ICMP Ping;

8. Ao concluir o passo 7, você terá dois hosts cadastrado, além do Zabbix server;

Nome	Aplicações	Itens	Triggers	Gráficos	Descoberta	Web	Interface	Templates	Status	Disponibilidade	Criptografia do
<input type="checkbox"/> pfsense	Aplicações 1	Itens 3	Triggers 3	Gráficos	Descoberta	Web	192.168.1.1: 10050	Template Module ICMP Ping	Ativo	ZBX SNMP JMX IPMI	NENHUM
<input type="checkbox"/> webserv	Aplicações 1	Itens 3	Triggers 3	Gráficos	Descoberta	Web	192.168.1.3: 10050	Template Module ICMP Ping	Ativo	ZBX SNMP JMX IPMI	NENHUM

9. Agora refaça os passo 5 e 6 para cadastrar os quatro **switchs** de rede, lembre-se de alterar as seguintes informações de acordo com cada equipamento, vide cenário:

- Seção Host:
- Nome do host: **VIDE CENÁRIO**
- Nome visível: **VIDE CENÁRIO**
- Grupos: Switchs (basta digitar para aparecer...)
- Interfaces do agente: **VIDE CENÁRIO**
- Seção Templates:
- Vincular a novos templates: digite icmp para pesquisar, escolha a opção Template Module ICMP Ping;

10. Agora refaça os passo 5 e 6 para cadastrar os três **access points** (APs), lembre-se de alterar as seguintes informações de acordo com cada equipamento, vide cenário:

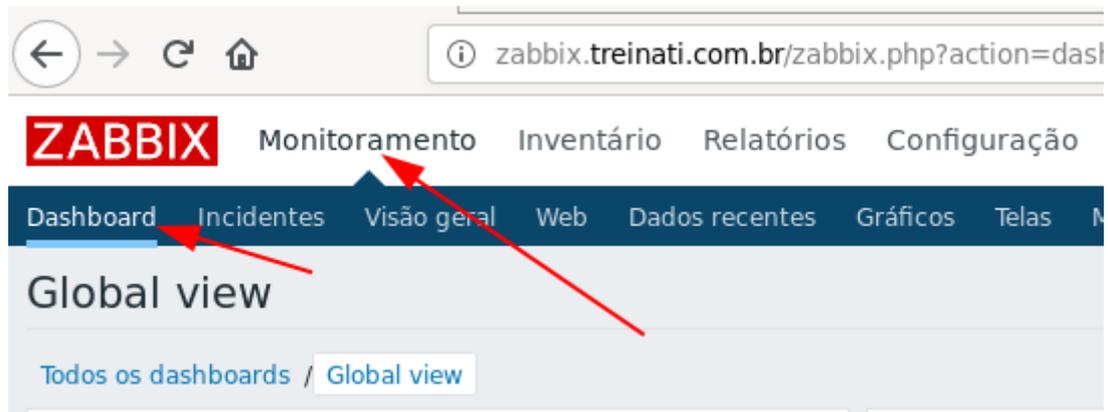
- Seção Host:
- Nome do host: **VIDE CENÁRIO**
- Nome visível: **VIDE CENÁRIO**
- Grupos: Access Points (basta digitar para aparecer...)
- Interfaces do agente: **VIDE CENÁRIO**
- Seção Templates:
- Vincular a novos templates: digite icmp para pesquisar, escolha a opção Template Module ICMP Ping;

11. Ao concluir os passos anteriores, você terá um total de 10 hosts cadastrados, são eles:

- 1 servidor zabbix;

- 2 servidores de rede;
- 4 switches de rede;
- 3 access points.

12. Para retornar à Dashboard, acesse: Monitoramento>Dashboard

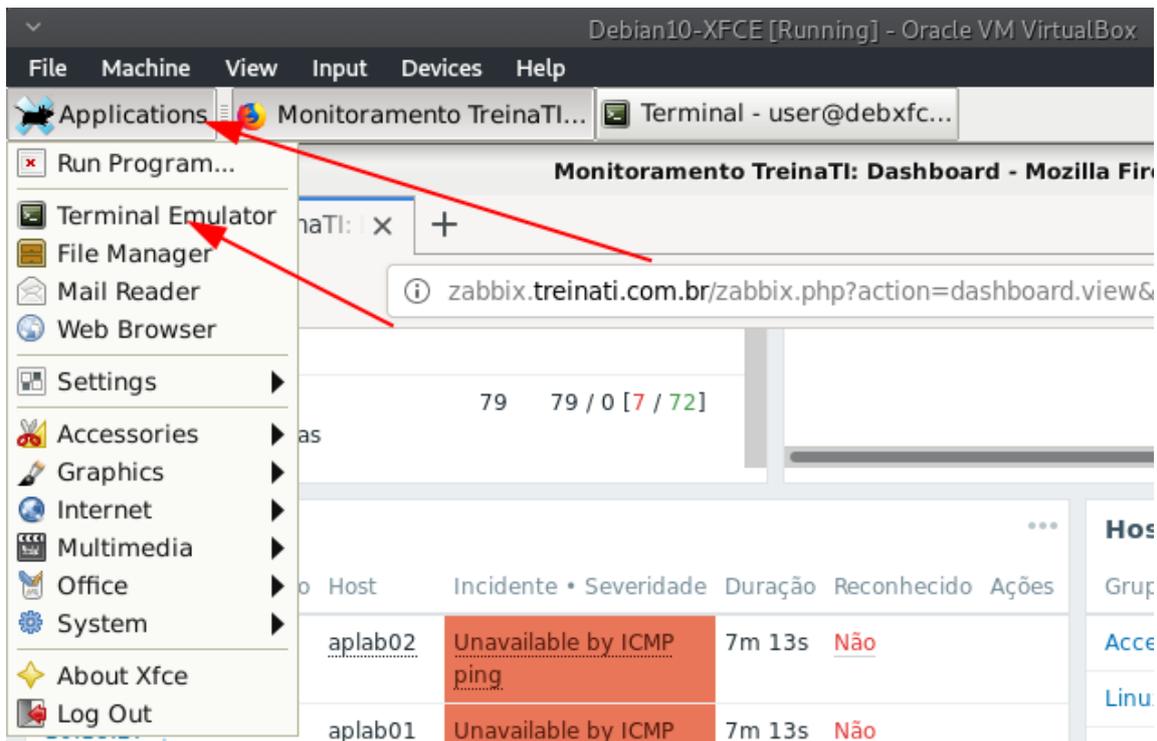


13. Observe que os switches e access points estão com incidentes:

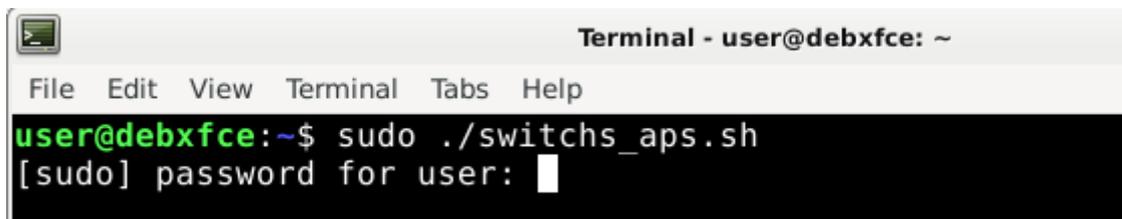
Incidentes							Hosts com problema			
Hora	Informação	Host	Incidente • Severidade	Duração	Reconhecido	Ações	Grupo de hosts	Sem incidentes	Com incidentes	Total
10:18:27		aplab02	Unavailable by ICMP ping	5m 13s	Não		Access Points		3	3
10:18:27		aplab01	Unavailable by ICMP ping	5m 13s	Não		Linux servers	2		2
10:17:27		apadm01	Unavailable by ICMP ping	6m 13s	Não		Switchs		4	4
10:17:24		swlabi01	Unavailable by ICMP ping	6m 16s	Não		Zabbix servers	1		1
10:16:26		swlabi02	Unavailable by ICMP ping	7m 14s	Não					
10:16:23		swadm01	Unavailable by ICMP ping	7m 17s	Não					
10:16:21		swdist01	Unavailable by ICMP ping	7m 19s	Não					

14. O incidente relatado no passo anterior se deve ao fato de que os equipamentos estão **desligados**. Para ligá-los, faça:

- Na VM Debian10-XFCE, acesse o menu: Applications>Terminal Emulador.



- No terminal que se abre, digite o seguinte comando: **sudo ./switchs_aps.sh**
- Será solicitada senha do usuário, digite: **qwe123**

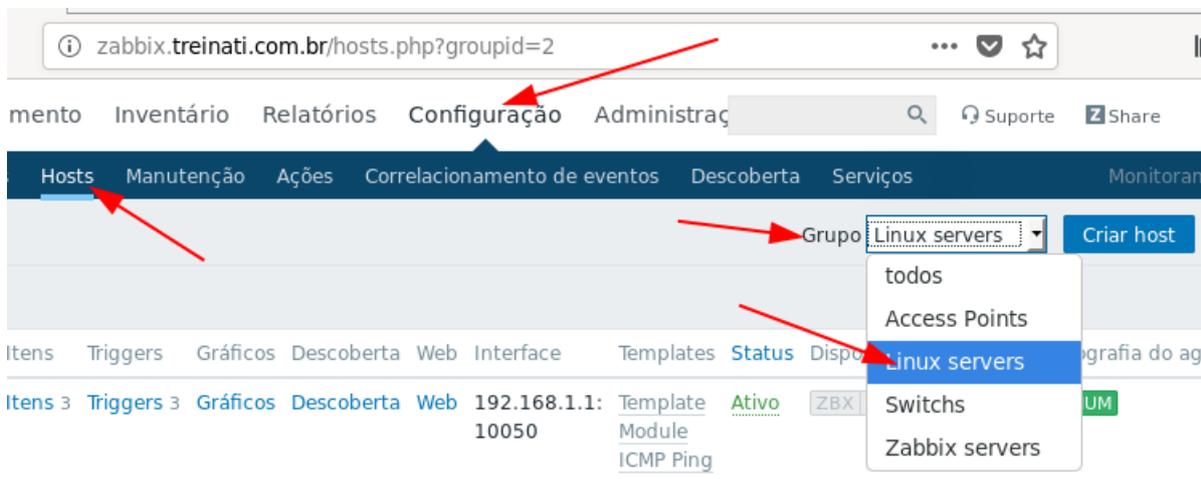


- Uma lista de opções será apresentada, cada opção liga ou desliga determinado equipamento do ambiente de rede da empresa. Para ligar todos os equipamentos de uma só vez digite a opção: **11** [tecle ENTER]
- Minimize a janela do terminal e verifique na Dashboard do Zabbix se os equipamentos estão online. Se necessário, atualize a página com **F5**!

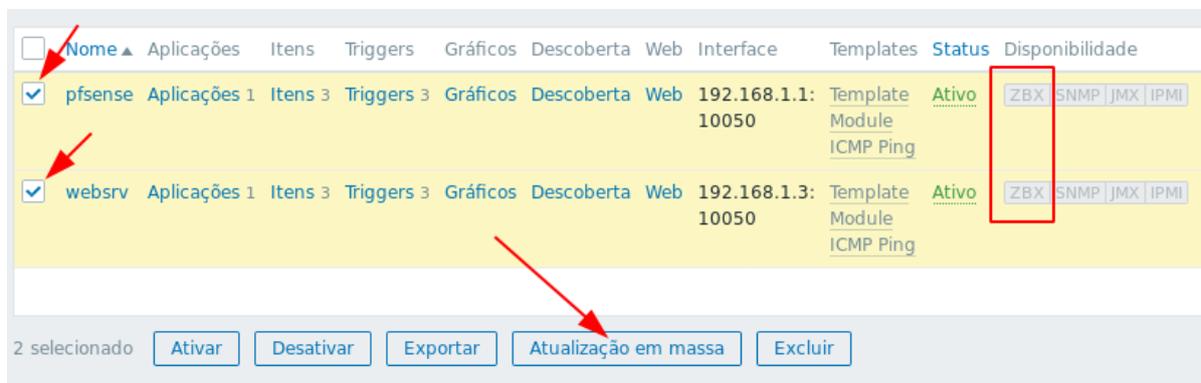
15. Pronto! Você já tem seu ambiente monitorado com a monitoração simples do Zabbix.

2. Monitorar os servidores com Zabbix Agent;

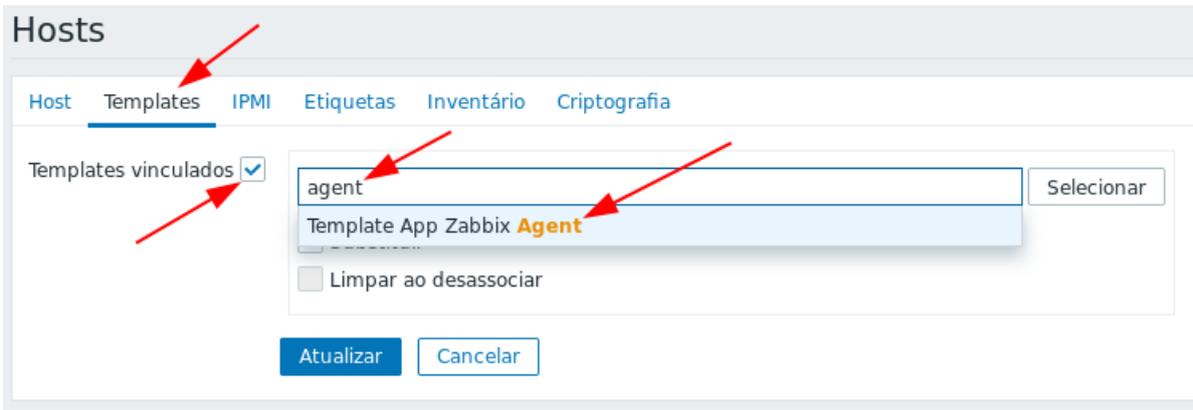
1. Diferente da monitoração simples, a monitoração com Zabbix Agent permite a coleta de informações dos hosts tais como uso do disco, uso de memória, uso da rede, uso do processador, entre vários itens possíveis. Para isso é necessário a instalação do Zabbix Agent nos servidores. Um ponto importante é que apenas servidores que possuam sistemas operacionais instalados (Linux, Windows, etc) é que podem utilizar o Zabbix Agent. No cenário atual temos dois hosts candidatos a utilização que são o servidor web (WebSRV) e o firewall (pfSense). Estes dois hosts já estão com o agente instalado, basta configurá-los no Zabbix.
2. Para configurar a monitoração via agente, acesse o menu: Configuração>Hosts; em seguida clique no Grupo e escolha "Linux servers";



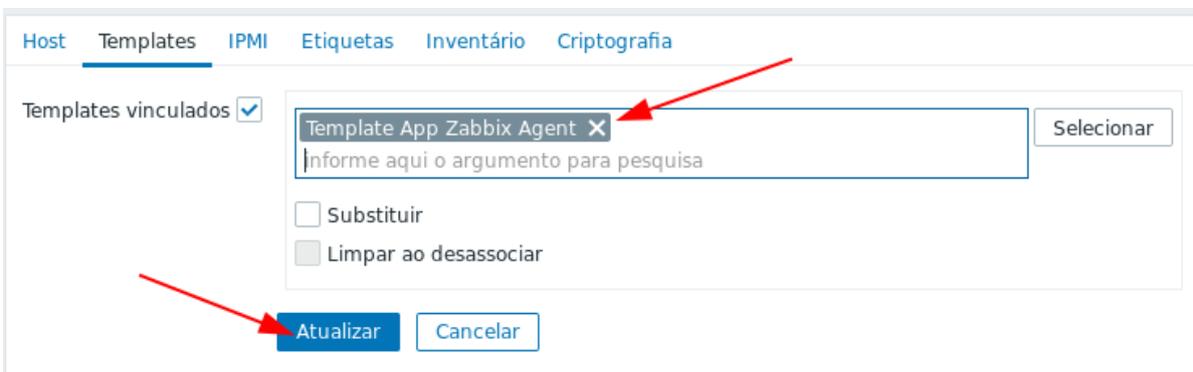
3. Será listado apenas os servidores linux configurados. Observem que eles não possuem agente configurado (ZBX). Selecione os dois e clique no botão "Atualização em massa";



4. Clique em Templates, marque Templates vinculados; pesquise por “agent” na seleção escolha a opção “Template App Zabbix Agent”;



5. Clique em Atualizar:



6. Aguarde um minuto aproximadamente até que ele atualize a ligação com o agente. Ficará como mostrado abaixo:

<input type="checkbox"/>	Nome	Aplicações	Itens	Triggers	Gráficos	Descoberta	Web	Interface	Templates	Status	Disponibilidade
<input type="checkbox"/>	pfsense	Aplicações 2	Itens 6	Triggers 6	Gráficos	Descoberta	Web	192.168.1.1:10050	Template App Zabbix Agent, Template Module ICMP Ping	Ativo	ZBX SNMP JMX IPMI
<input type="checkbox"/>	websrv	Aplicações 2	Itens 6	Triggers 6	Gráficos	Descoberta	Web	192.168.1.3:10050	Template App Zabbix Agent, Template Module ICMP Ping	Ativo	ZBX SNMP JMX IPMI

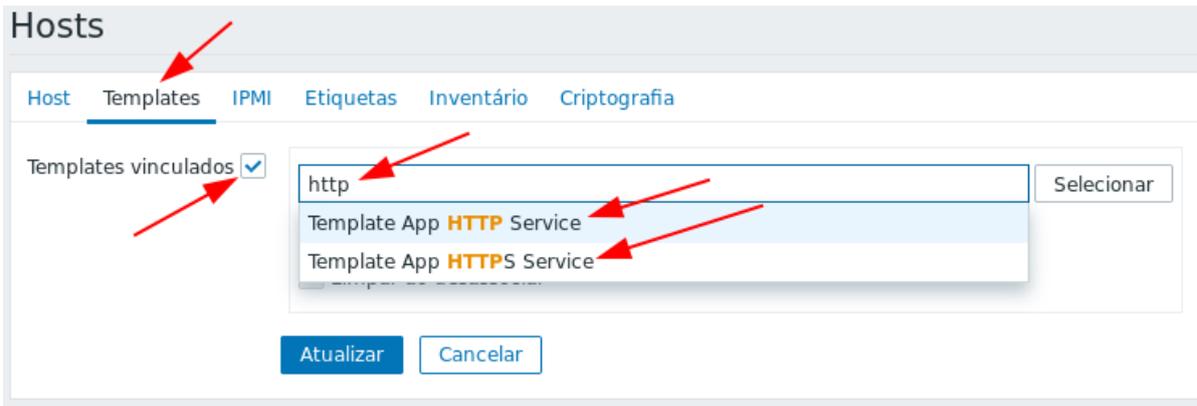
7. A partir de agora o Zabbix monitorará o servidor Linux mostrando dados dos seus periféricos instalados, de acordo com a configuração do Template associado.

3. Monitorar o serviço HTTP e HTTPS do servidor web;

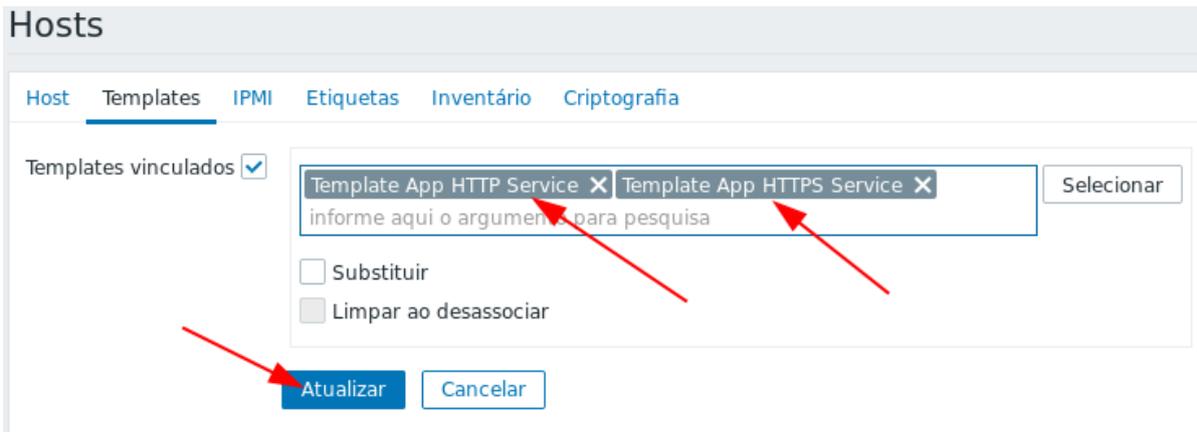
1. Para realizar a monitoração dos processos e serviços que estão em execução no servidor é necessária a instalação do Zabbix Agent. Neste cenário, o servidores que iremos utilizar já possuem o Zabbix Agent instalado e na atividade anterior (atividade 2) realizamos a ligação com o Zabbix Agent. Portanto, para realizar esta atividade de nº 3, faça antes a atividade 2!
2. Acesse: Configuração>Hosts; escolha no combo-box Grupo “Linux servers”; selecione os dois servidores; clique em “Atualização em massa”;

The screenshot displays the Zabbix web interface. The top navigation bar includes the ZABBIX logo and menu items: Monitoramento, Inventário, Relatórios, Configuração, and Administração. A search bar and a 'Suporte' link are also present. The sub-navigation bar shows: Grupos de hosts, Templates, Hosts, Manutenção, Ações, Correlacionamento de eventos, Descoberta, and Serviços. The main content area is titled 'Hosts' and features a dropdown menu for 'Grupo' set to 'Linux servers'. Below this is a table with columns: Nome, Aplicações, Itens, Triggers, Gráficos, Descoberta, Web, Interface, Templates, Status, and Disponibilidade. Two hosts are listed: 'pfsense' (IP 192.168.1.1:10050) and 'webserv' (IP 192.168.1.3:10050). Both have checkboxes selected. At the bottom, a status bar shows '2 selecionado' and buttons for 'Ativar', 'Desativar', 'Exportar', 'Atualização em massa', and 'Excluir'. Red arrows point to the 'Hosts' menu item, the 'Configuração' menu item, the 'Grupo' dropdown, the checkboxes for both hosts, and the 'Atualização em massa' button.

3. Clique em Templates; marque o check-box templates vinculados; digite para pesquisar “http”; selecione os dois templates que aparecerão: “Template App HTTP Service” e “Template App HTTPS Service”;



4. Adicionado os templates, clique em Atualizar;



5. Após atualizar, aguarde a sincronização. Para verificar os dados coletados, acesse: Monitoramento>Visão geral;

ZABBIX Monitoramento Inventário Relatórios Configuração Administração

Dashboard Incidentes Visão geral Web Dados recentes Gráficos Telas Mapas Descoberta Serviços Monitoramento TreinaTI

Visão geral Grupo Linux servers Tipo Dados Localização dos hosts Esquerda

Filtrar

Hosts	Host name of Zabbix agent running	HTTP service is running	HTTPS service is running	ICMP loss	ICMP ping	ICMP response time	Version of Zabbix agent running	Zabbix agent ping
pfsense	pfsense	Up (1)	Up (1)	0 %	Up (1)	0.7ms	4.2.1	Up (1)
websrv	websrv	Up (1)	Up (1)	0 %	Up (1)	0.7ms	4.2.6	Up (1)

4. Monitorar os portais de serviço (Site e Moodle) da empresa.

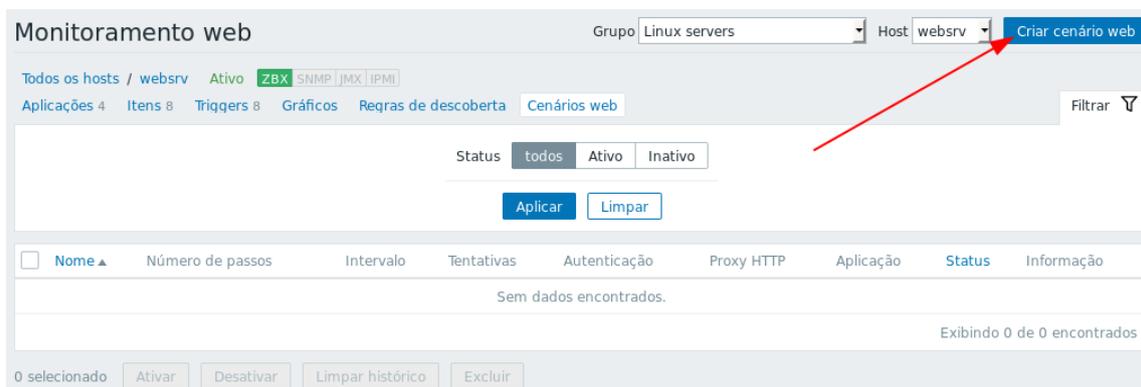
1. Com a monitoração web podemos verificar velocidade de download por segundo, tempo de resposta, código de resposta de determinado site na web. Aqui vamos criar dois cenários web: um para o portal da empresa e outro para o Moodle.

2. Cenário web para o Portal e o Moodle da empresa:

1. Acesse: Configuração>Hosts. Localize o host **webserv** e clique no link “Web”;



2. Clique no botão “Criar cenário web”



3. Na aba Cenário, preencha os campos como mostrado na imagem abaixo:

Cenário **Passos** Autenticação

* Nome Portal Web

Aplicação

Nova aplicação Web checks

* Intervalo de atualização 1m

* Tentativas 1

Agente Firefox 33.0 (Linux)

Proxy HTTP [protocol://][user[:password]@]proxy.example.com[:port]

Variáveis

Nome	Valor	
nome	valor	Remove

Adicionar

Cabeçalhos

Nome	Valor	
nome	valor	Remove

Adicionar

Ativo

4. Na aba Passos, clique no link “Adicionar”:

Cenário **Passos** Autenticação

* Passos

Nome	Tempo limite	URL
Adicionar		

Adicionar Cancelar

5. Preencha os campos como mostrado na imagem abaixo (campos vazios deixe como está) ao final clique em “Adicionar”:

Passo do cenário web

* Nome Home

* URL http://www.treinati.com.br Processar

Campos da consulta

Nome	Valor	
nome	valor	Remove

Adicionar

Seguir redirecionamentos

Modo de busca **Corpo** Cabeçalhos Corpo e cabeçalhos

* Tempo limite 15s

Texto requerido

Código de status requerido 200

Atualizar Cancelar

6. Adicione um segundo passo para o Site, clique no link novamente em “Adicionar”:

Cenário Passos Autenticação

* Passos	Nome	Tempo limite	URL	Requerido	Códigos de status	Ação
1:	Home	15s	http://www.treinati.com.br/			Remover

[Adicionar](#)

Adicionar Cancelar

7. Preencha os campos como mostrado na imagem abaixo (campos vazios deixe como está) ao final clique em “Adicionar”:

Passo do cenário web

* Nome Administrator

* URL http://www.treinati.com.br/administrator/ **Processar**

Campos da consulta

Nome	Valor	
nome	⇒	valor Remover

[Adicionar](#)

Seguir redirecionamentos

Modo de busca **Corpo** Cabeçalhos Corpo e cabeçalhos

* Tempo limite 15s

Texto requerido

Código de status requerido 200

Atualizar Cancelar

8. Após adicionar os passos, clique no botão “Adicionar” para concluir o cenário do Portal Web:

Cenário Passos Autenticação

* Passos

Nome	Tempo limite	URL	Requerido	Códigos de status	Ação
1: Home	15s	http://www.treinati.com.br/			Remover
2: Administrator	15s	http://www.treinati.com.br/administrator/			Remover

[Adicionar](#)

Adicionar Cancelar

9. Refaça os passos anteriores, dessa vez utilize o Moodle para monitoramento do cenário web, clique no botão “Criar cenário web”, preencha como abaixo:

Cenário Passos Autenticação

* Nome Moodle

Aplicação

Nova aplicação Web checks

* Intervalo de atualização 1m

* Tentativas 1

Agente Firefox 33.0 (Linux)

Proxy HTTP [protocol://][user[:password]@]proxy.example.com[:port]

Variáveis

Nome	Valor	
nome	valor	Remove

[Adicionar](#)

Cabeçalhos

Nome	Valor	
nome	valor	Remove

[Adicionar](#)

Ativo

10. Clique na aba “Passos”, em seguida no link “Adicionar”

Cenário Passos Autenticação

* Passos

Nome	Tempo limite	URL
Adicionar		

[Adicionar](#) [Cancelar](#)

11. Preencha como mostrado abaixo e clique em “Adicionar”:

Passo do cenário web

* Nome Home

* URL http://moodle.treinati.com.br [Processar](#)

Campos da consulta

Nome	Valor	
nome	valor	Remove

[Adicionar](#)

Seguir redirecionamentos

Modo de busca **Corpo** Cabeçalhos Corpo e cabeçalhos

* Tempo limite 15s

Texto requerido

Código de status requerido 200

Atualizar Cancelar

12. Adicione um segundo passo para o Moodle:

Cenário Passos Autenticação

* Passos

Nome	Tempo limite	URL	Requerido	Códigos de status	Ação
1: Home	15s	http://moodle.treinati.com.br			Remover

[Adicionar](#)

Adicionar Cancelar

13. Preencha como mostrado abaixo:

Passo do cenário web

* Nome Moodle Login

* URL http://www.treinati.com.br/moodle/login/index.php **Processar**

Campos da consulta

Nome	Valor	Ação
nome	valor	Remover

[Adicionar](#)

Seguir redirecionamentos

Modo de busca **Corpo** Cabeçalhos Corpo e cabeçalhos

* Tempo limite 15s

Texto requerido

Código de status requerido 200

Atualizar Cancelar

14. Ao final, clique em “Adicionar” para concluir o cenário web:

Nome	Tempo limite	URL	Requerido	Códigos de status	Ação
1: Home	15s	http://moodle.treinati.com.br			Remover
2: Moodle Login	15s	http://www.treinati.com.br/moodle/login/index.php			Remover

[Adicionar](#)

15. Ao finalizar os cenários web, você terá algo como mostrado abaixo:

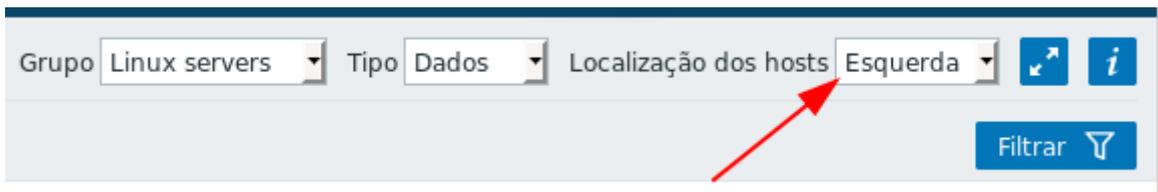
Nome	Número de passos	Intervalo	Tentativas	Autenticação	Proxy HTTP	Aplicação	Status	Informação
Moodle	2	1m	1	Nenhum	Não	Web checks	Ativo	
Portal Web	2	1m	1	Nenhum	Não	Web checks	Ativo	

Exibindo 2 de 2 encontrados

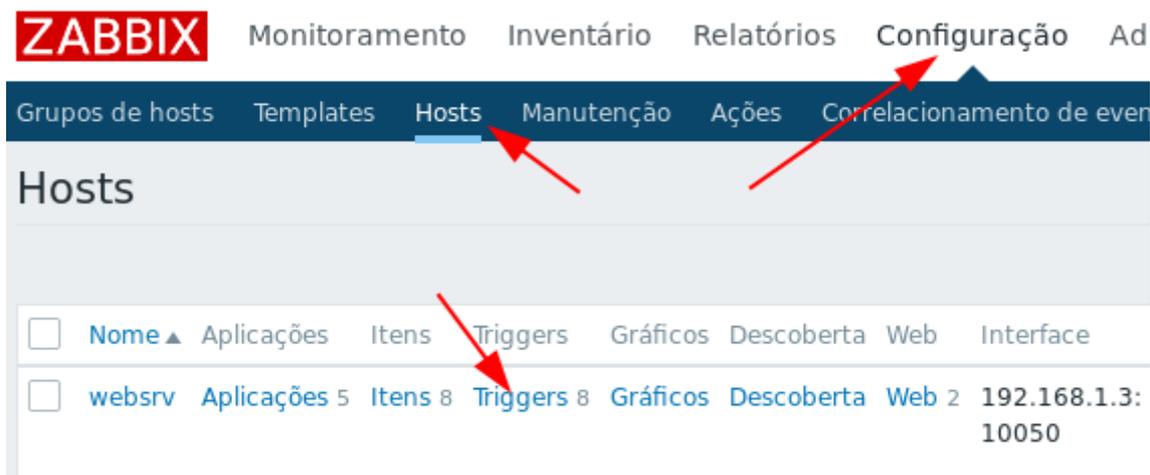
16. Para verificar os dados coletados, acesse: Monitoramento>Visão geral:

Hosts	Download speed for scenario "Moodle".	Download speed for scenario "Portal Web".	Download speed for step "Administrator" of scenario "Portal Web".	Download speed for step "Home" of scenario "Moodle".	Download speed for step "Home" of scenario "Portal Web".	Download speed for step "Moodle Login" of scenario "Moodle".	Failed step of scenario "Moodle".	Failed step of scenario "Portal Web".	Host name of Zabbix agent running	HTTP service is running	HTTPS service is running	ICMP loss	ICMP ping	ICMP response time	Last error message of scenario "Moodle".	Last error message of scenario "Portal Web".	Response code for step "Administrator" of scenario "Portal Web".	Response code for step "Home" of scenario "Moodle".
webserv	1.27 MBps	244.5 KBps	363.49 KBps	286.8 KBps	125.52 KBps	2.26 MBps	0	0	webserv	Up (1)	Up (1)	0 %	Up (1)	0.6ms			200	200

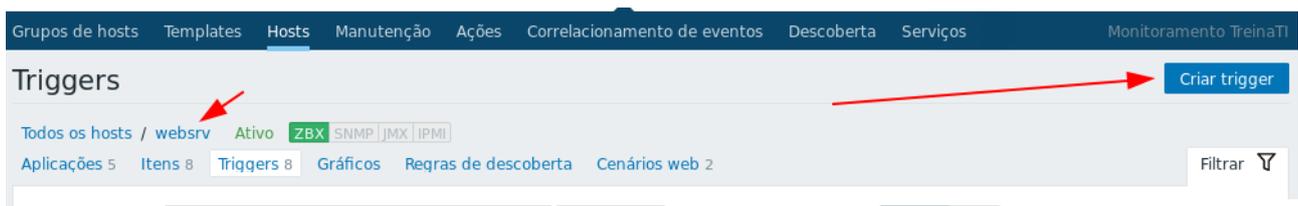
17. Se desejar uma melhor visualização, altere a localização dos hosts no menu superior, altere como achar melhor:



3. Vamos criar as *triggers* para os dois cenários web. Elas serão responsáveis por inserir um alerta na Dashboard do Zabbix. Acesse: Configuração>Hosts; clique no link “Triggers” do host webserv;



4. Clique no botão “Criar trigger”:



5. Insira as informações conforme abaixo para a trigger do Portal Web:

- Nome: Falha Portal Web
- Severidade: Alta
- Expressão: {webserv:web.test.fail[Portal Web].last()}=1
- Clique em Adicionar.

Trigger **Etiquetas** Dependências

* Nome Falha Portal Web

Severidade Não classificada Informação Atenção Média **Alta** Desastre

* Expressão {webserv:web.test.fail[Portal Web].last()}=1 Adicionar

[Construtor de expressão](#)

6. Clique novamente no botão “Criar trigger”. Insira as informações conforme abaixo para a trigger do Moodle:

1. Nome: Falha Moodle
2. Severidade: Alta
3. Expressão: {webserv:web.test.fail[Moodle].last()}=1
4. Clique em Adicionar.

Trigger **Etiquetas** Dependências

* Nome Falha Moodle

Severidade Não classificada Informação Atenção Média **Alta** Desastre

* Expressão {webserv:web.test.fail[Moodle].last()}=1 Adicionar

[Construtor de expressão](#)

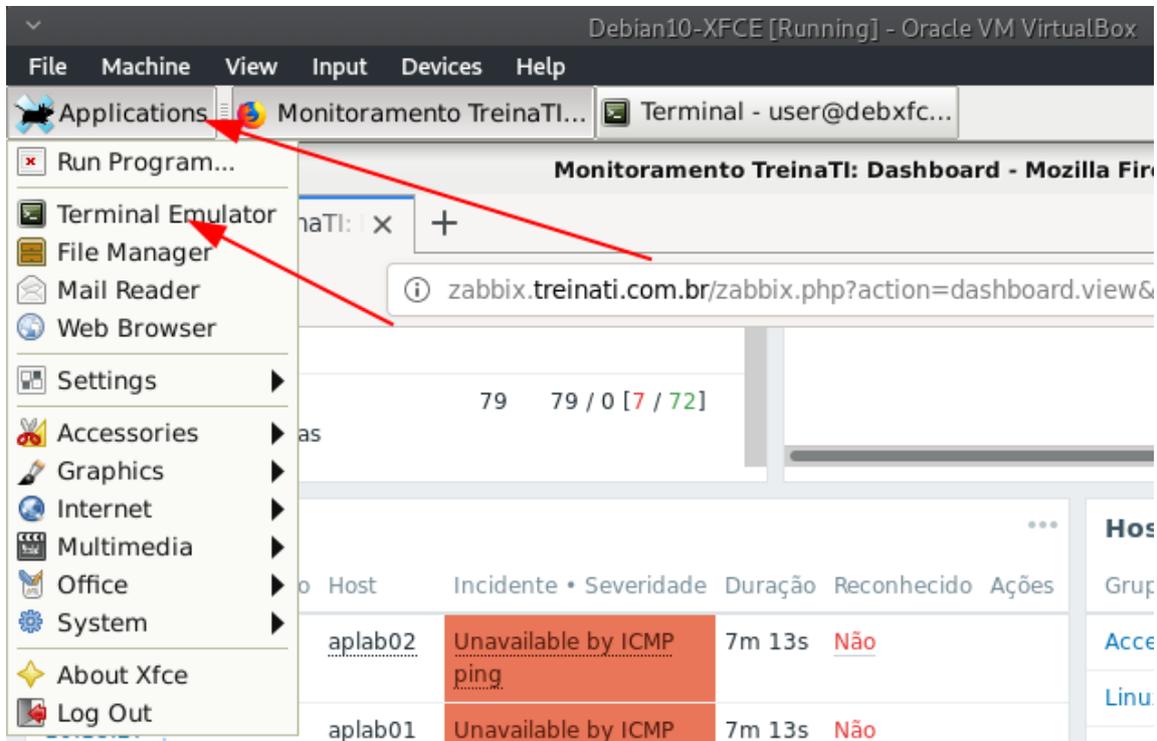
7. Ao final você terá duas triggers:

<input type="checkbox"/>	Severidade	Valor	Nome ▲	Expressão	Status
<input type="checkbox"/>	Alta	OK	Falha Moodle	{webserv:web.test.fail[Moodle].last()}=1	Ativo
<input type="checkbox"/>	Alta	OK	Falha Portal Web	{webserv:web.test.fail[Portal Web].last()}=1	Ativo

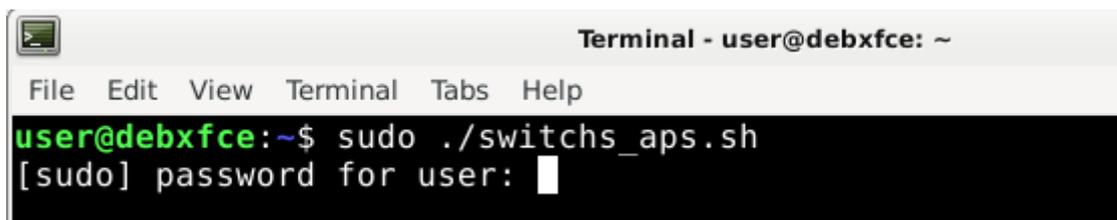
Simulando falhas

Simular Falha de comunicação com Switch e AP:

- Na VM Debian10-XFCE, acesse o menu: Applications>Terminal Emulator.



- No terminal que se abre, digite o seguinte comando: **sudo ./switchs_aps.sh**
- Caso seja solicitada senha do usuário, digite: **qwe123**



- Uma lista de opções será apresentada, cada opção liga ou desliga determinado equipamento do ambiente de rede da empresa. Para desligar o switch administrativo digite a opção: **30** [tecle ENTER]
- Minimize a janela do terminal e verifique na Dashboard do Zabbix se os equipamentos estão offline. Se necessário, atualize a página com **F5**!

Incidentes						
Hora ▼	Informação	Host	Incidente • Severidade	Duração	Reconhecido	Ações
14:16:26		apadm01	Unavailable by ICMP ping	17s	Não	
14:16:23		swadm01	Unavailable by ICMP ping	20s	Não	

- Para religar o equipamento, escolha a opção: **31** [tecle ENTER]

Simular Falha na aplicação Apache2 (HTTP e HTTPS):

Com o terminal aberto, conecte-se remotamente via SSH ao servidor web com o seguinte comando:

- `ssh user@treinati.com.br`

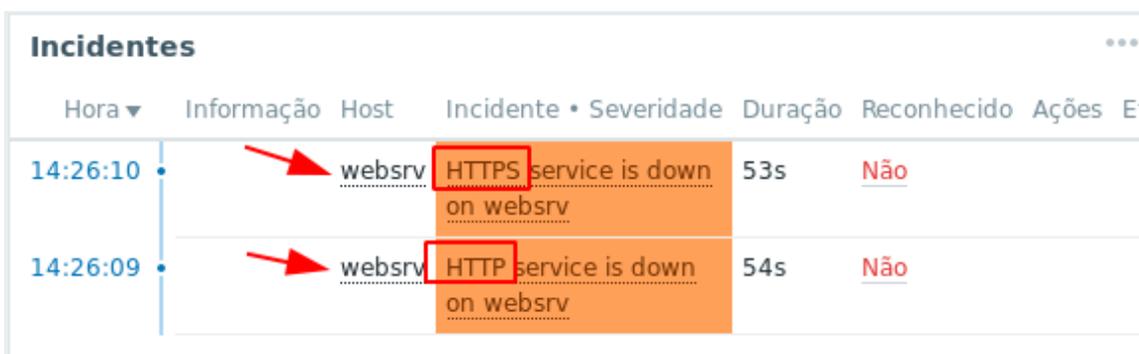
Será solicitada a senha, informe: **qwe123**

Agora você está logado remotamente ao servidor web. Para simular a falha na aplicação vamos parar o serviço do apache2. Use o seguinte comando:

- `sudo systemctl stop httpd`

Será solicitada a senha, informe: **qwe123**

Verifique na Dashboard do Zabbix se apareceu o alerta. Você também pode verificar através da opção Monitoramento>Visão geral.



Hora	Informação	Host	Incidente • Severidade	Duração	Reconhecido	Ações	Et
14:26:10		webserv	HTTPS service is down on webserv	53s	Não		
14:26:09		webserv	HTTP service is down on webserv	54s	Não		

Para restabelecer o serviço, execute o comando:

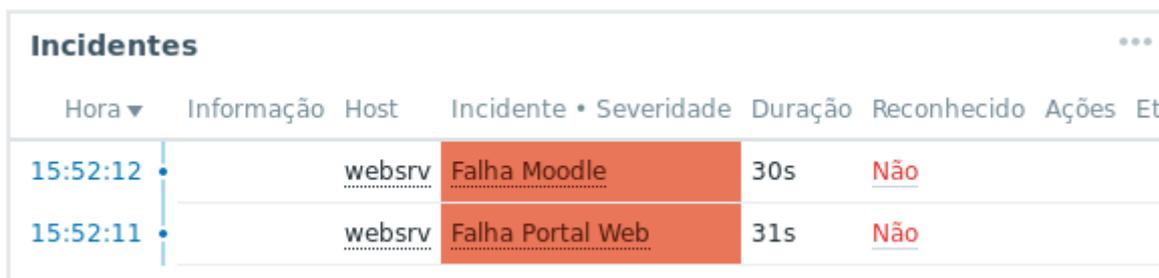
- `sudo systemctl start httpd`

Simular Falha no acesso aos portais Site e Moodle:

Ainda logado no servidor web execute os comandos para colocar o site offline:

- `cd /etc/httpd/conf.d/`
- `sudo mv www.treinati.conf /root/`
- `sudo systemctl restart httpd`

Verifique na Dashboard do Zabbix o alerta.



Hora	Informação	Host	Incidente • Severidade	Duração	Reconhecido	Ações	Et
15:52:12		webserv	Falha Moodle	30s	Não		
15:52:11		webserv	Falha Portal Web	31s	Não		

Para colocar o site novamente online, execute os comandos no servidor web:

- `sudo mv /root/www.treinati.conf ./`
- `sudo systemctl restart httpd`

Verifique na Dashboard do Zabbix se o alerta sumiu.

Referências:

- I. https://zabbix.org/wiki/Main_Page
- II. <https://www.zabbix.com/manuals>