

MANUAL DE UTILIZAÇÃO DO SISTEMA ZABBIX PARA USUÁRIOS

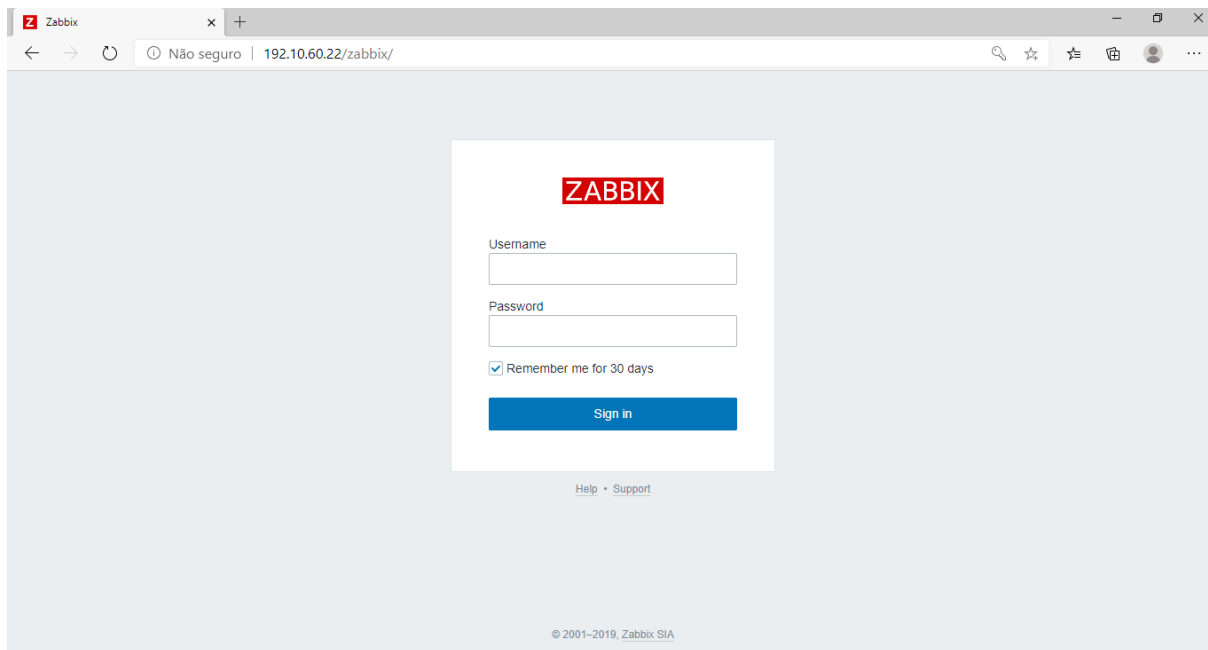
ZABBIX
MONITORING SYSTEM



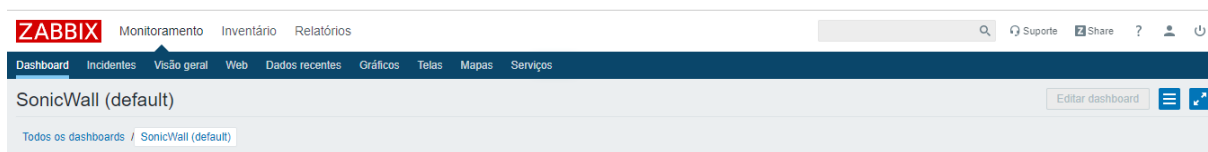
Junho/2020

1. COMO ACESSAR O SISTEMA

Para acessar o sistema abra seu navegador de preferência e acesse: <http://192.10.60.22/zabbix>. Insira seu usuário e senha e acesse o sistema. O usuário e senha é gerado pelo administrador do sistema, se você ainda não tem acesso entre em contato com TI-INFRA.



2. NAVEGAÇÃO PELO SISTEMA



A navegação pelo sistema é feita através da barra superior. E a primeiro momento os três campos que terão utilidade estão na barra inferior de “Monitoramento”: Dashboards, Dados Recentes e Incidentes.

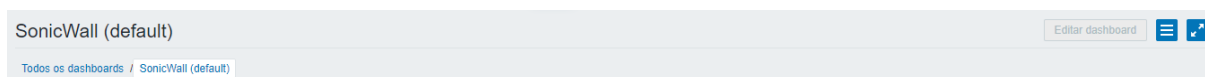


Junho/2020

3. DASHBOARD

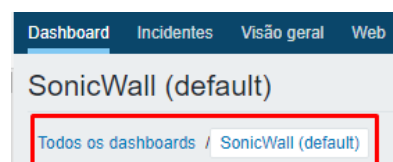
3.1 INTRODUÇÃO

Ao clicar em monitoramento e logo em baixo Dashboard o usuário é redirecionado para página configurada como padrão ou para o último dashboard que ele utilizou.

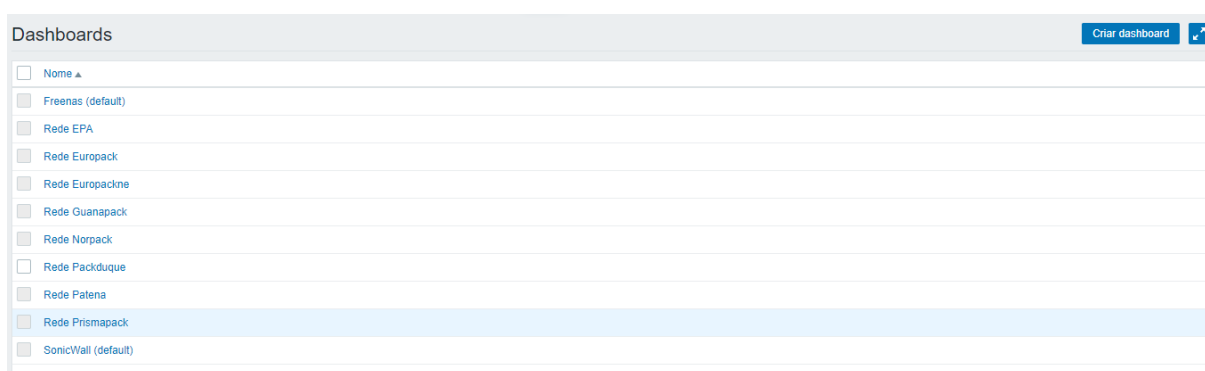


Logo abaixo tem o nome do dashboard visualizado, neste exemplo *SonicWall (default)* e a direita tem dois ícones, o primeiro é chamado ícone de ações, serve para criar um dashboard exclusivo para seu usuário, e o segundo é o ícone para deixar o dashboard selecionado em tela cheia.

Abaixo do nome do dashboard visualizado que está na cor preta e em uma fonte maior, temos uma espécie de caminho formado por *todos os dashboards / dashboard selecionado*.



Ao clicar em Todos os dashboards o usuário pode ver todos os dashboards que ele tem permissão de visualizar. Por padrão cada helpdesk tem acesso ao dashboard de sua unidade e o grupo adm_tic pode visualizar todos os dashboards das unidades + SonicWall (default) e Freenas (default).



A direita repete-se a mesma coisa que vimos no começo, um botão para criar um dashboard privado e outro para colocar em tela cheia.



Junho/2020

3.2 VISÃO GERAL DA UNIDADE

Ao selecionar uma Rede + Unidade qualquer abrirá o dashboard da unidade. Um dashboard não é exatamente igual aos outros porque algumas unidades tem uma necessidade de monitorar a latência com o servidor da cisco através do <https://mediatest.ciscospark.com/#!/main> devido ao equipamento de videoconferência, enquanto que outras não. Assim a forma de distribuição dos gráficos na tela pode variar para cada unidade.

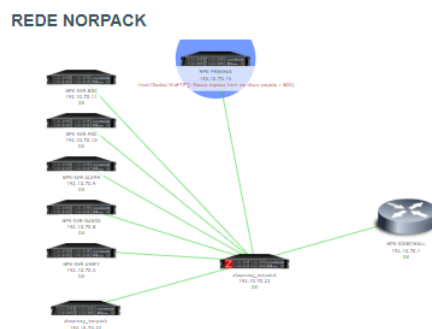
De modo global são monitorados nas unidades por servidor: monitoramento cpu, monitoramento de discos, monitoramento de memória, monitoramento do espaço em disco do Freenas e o status do ping. Para o roteador SonicWall é monitorado entrada/saída e status das portas que são utilizadas pelos links dos provedores em cada unidade (x1,x2...). Por unidade é monitorado a latência para o servidor MySQL e a disponibilidade de banda que é uma consulta ao <https://www.speedtest.net/>.

3.2 ELEMENTOS DASHBOARD DE UMA UNIDADE

3.2.1 Mapa

Em todos os dashboards das unidades temos um mapa. Este mapa não corresponde a forma física montada no rack da unidade, obviamente, mas ele tem a função de ajudar quem está observando identificar em qual servidor pode estar ocorrendo algum incidente.

Incidentes estão divididos em 6 categorias por gravidade: 1) Não classificada; 2) informação; 3) atenção; 4) média; 5) alta; 6) desastre.



Como se pode ver no dashboard da Rede Norpack temos um incidente ocorrendo. A cor azul é característica de uma informação, amarelo ouro atenção, laranja média, vermelho claro alta e vermelho escuro desastre.

Temos um incidente na Norpack. Vejamos com mais detalhes no próximo widget.

3.2.2 Incidentes

Incidentes								
Hora ▼	Hora da recuperação	Status	Informação	Host	Incidente • Severidade	Duração	Reconhecido	Ações
04-06-2020 20:45:08		INCIDENTE		NPK-FREENAS	/mnt/Dados/ViaFTP": Pouco espaço livre no disco (usado > 60%)	4d 11h 2m	Não	

Em todas unidades temos um widget de incidentes. Ele está no topo pois através dele que podemos ver os detalhes de forma legível de uma trigger que foi disparada indicando um incidente que pode estar ocorrendo.

O widget de incidente contém: hora, hora da recuperação, status, informação, host, incidente-severidade, duração, reconhecido e ações.

Podemos ver na hora que no dia 04/06/2020 as 20:45:08 foi disparado um incidente, o host foi Freenas da Norpack (vale ressaltar que os dashboards das unidades estão limitados a mostrar somente o incidente que ocorre nela), sabemos que a cor azul representa uma informação, e está é que existe pouco espaço livre no disco (usado > 60%). O diretório /mnt/Dados/ViaFTP é o local onde está armazenado os dados de backup gravados via ftp no Freenas.

Não é necessário entrar em pânico ao ver um incidente. A exemplo dos Freenas, está configurado 3 triggers para nos avisar. Primeiro um trigger de informação é disparado quando o espaço em disco passa de 60%, a segunda trigger configurado como alta ocorre quando o espaço em disco passa de 90%, neste momento requer que alguém limpe os backups antigos e caso o responsável se passe,



Junho/2020

está configurado uma trigger de desastre, esta é disparada quando o espaço em disco passa de 98%.

Desastre	{#FSNAME}": Disco lotado (usado > 98%)
Alta	{#FSNAME}": Espaço livre em disco extremamente baixo (usado > 90%)
Informação	{#FSNAME}": Pouco espaço livre no disco (usado > 60%)

Duração mostra quanto tempo aquele incidente ficou ativo, essa informação é muito útil se quisermos fazer relatório.

Reconhecido permite ao usuário enviar uma mensagem quanto ao problema, mudar a severidade do incidente e terminar o problema. Estes últimos dois só é permitido no momento ao administrador.

Problema de atualização

Mensagem

okokokokokk

Histórico

Hora Usuário Ação do usuário Mensagem

Escopo

☒ Apenas o incidente selecionado
☐ Selecionado e todos os outros problemas de triggers relacionadas 1 evento

Mudar severidade

☐ Não classificada ☐ Informação ☐ Atenção ☐ Média ☐ Alta ☐ Desastre

Reconhecer

☒

Terminar incidente

☐

* É obrigatória uma operação de atualização ou mensagem.



Atualizar

Cancelar

Ao reconhecer o problema é disparado um e-mail avisando que um usuário reconheceu o problema e a mensagem que ele enviou:



Junho/2020

 Responder  Responder a Todos  Encaminhar



ter 09/06/2020 08:56

packinggroupzabbix@gmail.com

Atualização do problema 13286: /mnt/Dados/ViaFTP": Pouco espaço livre no disco (usado > 60%) (NPK-FREENAS • 192.10.70.15)

Para packinggroupzabbix@gmail.com

Renan Rodrigues (renan.rodrigues) acknowledged and commented problema às 2020.06.09 08:56:25.
okokokokokk

O atual status do problema é PROBLEM, conhecimento: Yes.

E por fim ações. Está configurado duas ações globais quando ocorrer um incidente, a primeira é disparar um email para packinggroupzabbix@gmail.com que redirecionará para lista de transmissão zabbix@packinggroup.com.br, e a segunda é enviar uma mensagem através de um bot para um grupo no Telegram.

Este é um exemplo de e-mail recebido. O título contém o ID do incidente, o nome do servidor e o IP, na mensagem demos o nome do problema, host, ip, gravidade.

 Responder  Responder a Todos  Encaminhar



ter 09/06/2020 08:37

packinggroupzabbix@gmail.com

Problema 14074: EUN-SVR-FREENAS • 192.10.20.15

Para packinggroupzabbix@gmail.com

Problema iniciado as 08:36:35 de 2020.06.09

Nome do Problema: /mnt/Dados/ViaFTP": Espaço livre em disco extremamente baixo (usado > 90%)

Host: EUN-SVR-FREENAS

IP: 192.10.20.15

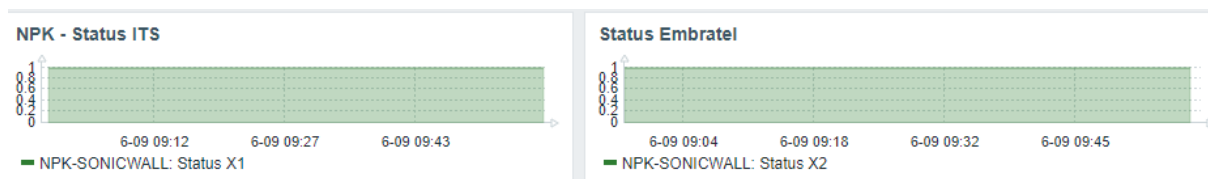
Gravidade: High

ID Problema: 14074



Junho/2020

3.2.3 Status Link Operadora



Através de uma consulta snmp ao SonicWall ele me retorna o status do link na porta do roteador. Em todas unidades tem configurado esse widget. Enquanto chega sinal na porta o status retorna 1 e caso pare o sinal o gráfico altera para 0.

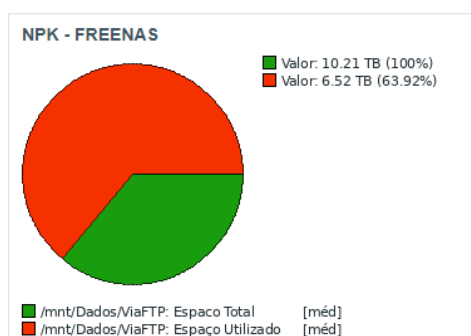
Normalmente para o sinal quando o link da operadora rompe ou quando se tira o cabo da porta do roteador. Caso isso ocorra será disparado uma trigger com a severidade de desastre.

Desastre	OK	Link Algar Não Responde
Desastre	OK	Link Embratel Não Responde

3.2.4 Freenas

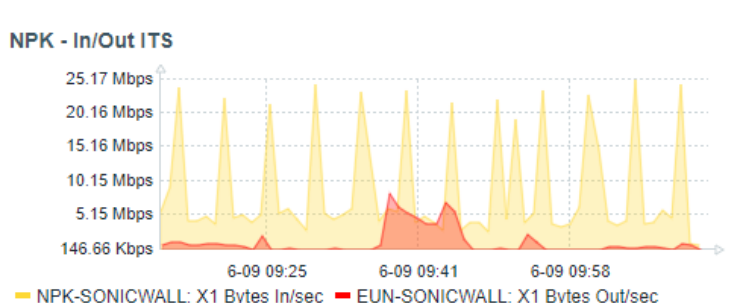
Esse widget também existe em todas as unidades. De modo objetivo este gráfico pizza mostra a relação entre o espaço utilizado, em vermelho, e o espaço livre em verde.

Já vimos que existem três triggers cadastradas para o Freenas quanto a espaço: 60, 90 e 98 sendo sua gravidade de informação, alta e desastre respectivamente.



3.2.5 In/Out Link

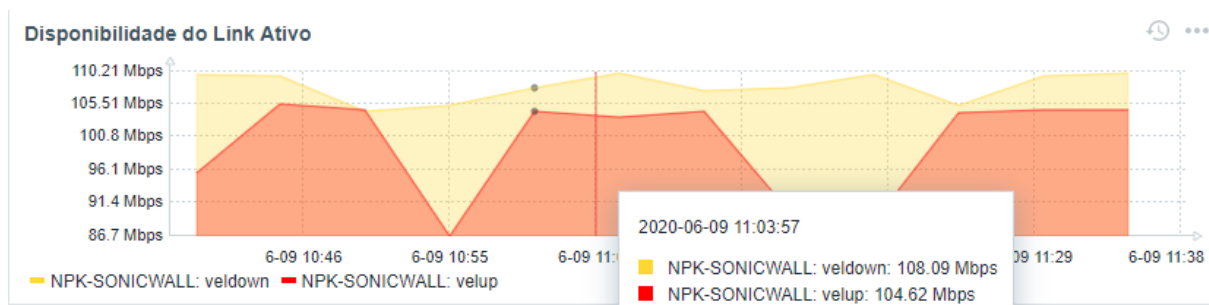
Através do protocolo SNMP também é obtido a quantidade de bits que trafega na porta do SonicWall. Este widget mostra estes dados, em



Junho/2020

amarelo temos a quantidade de bits que entra no roteador, download, e em vermelho o que sai, upload.

3.2.6 Disponibilidade do Link Ativo



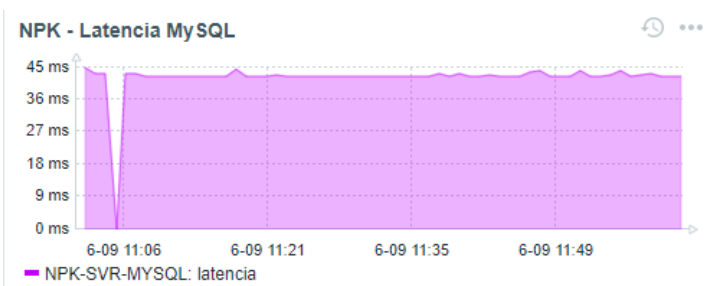
Este widget é uma consulta automatizada ao SpeedTest. Em todas as unidades exceto Europack ele é uma chamada a API do site e na Europack ela é um Web Scrapping de <https://www.speedtest.net/>. De toda forma a cada 10 minutos é executado o script que busca estes dados e envia para o Zabbix Server.

Durante o desenvolvimento foi identificado que uma consulta ao SpeedTest eleva o consumo de banda em 10 segundos para upload e mais 10 segundos para download. Após testes ficou ideal uma consulta feita a cada 10 minutos ou 600 segundos pois não gera impactos na rede.

O padrão de cores segue o mesmo padrão visto anteriormente. Amarelo é download e vermelho upload.

3.2.7 Latência MySQL

Este widget está presente em todas as unidades ele é o tempo de resposta de um ping para o ip do servidor onde está o MySQL. Atualmente o script gera vários falsos positivos



pois como é executado 1 ping a cada minuto por vezes o pacote ICMP se perde e a latência ultrapassa o limite definido no trigger.



Junho/2020

Atualmente o trigger está definido para disparar caso em 2 consultas o valor respondido seja

Severidade	Valor	Nome
Atenção	OK	Latencia alta (tempo resposta > 200 ms)
Alta	INCIDENTE	Servidor MySQL nao responde

maior que 200 milissegundos, neste caso identifica latência alta, porém se retornar 0 por duas vezes ele dispara que o servidor não está respondendo.

Devo fazer em breve (12/06/2020) uma melhoria no código para evitar falso-positivo. Sendo assim até o momento caso aparece uma mensagem de que a latência está muito alta não é necessária uma tomada de decisão no exato momento, mas se este erro permanecer por dois ou três minutos então deve ser tomada uma providência.

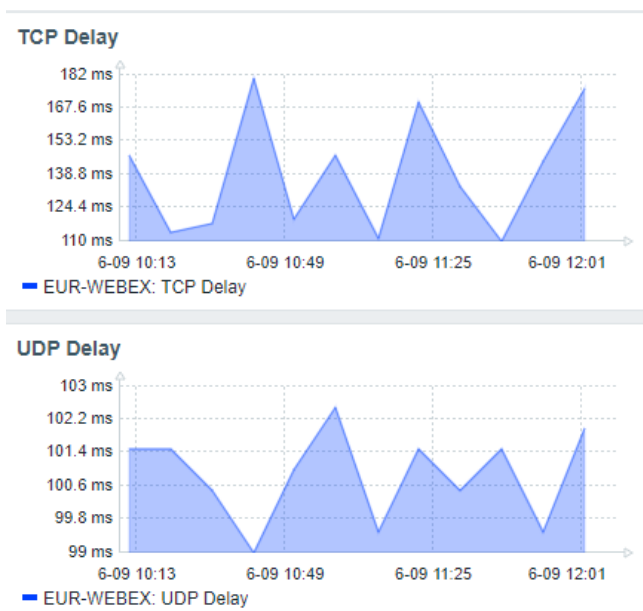
3.2.8 TCP/UDP Delay

Esta é uma consulta feita a cada 10 minutos a página <https://mediatest.ciscospark.com/>.

Sobre esse script vale a pena ressaltar que o resultado dele serve para nos dar noção de como está nossa conexão com o site da Cisco, porém os equipamentos de videoconferência possuem uma conexão dedicada pelo SonicWall.

Como na latência ao MySQL ninguém deve desesperar-se

caso em algum momento uma consulta chegue a 0 pois este valor eu coloquei como o padrão de retorno caso aconteça algum erro de comunicação. O script escrito em Python que fiz abre o motor do Firefox (sem a parte gráfica) executa todo o processo do site como faria qualquer ser humano, navega entre os elementos da “página” e retorna os valores obtidos. Porém pode acontecer uma falha na comunicação com site do Cisco ou por algum momento raro a consulta demorar mais de 1 minuto e 30 segundos definido como parâmetro para o script aguardar depois do start (botao que



Junho/2020

aparece para iniciar quando abre o site do mediatest) e antes da navegação. Enquanto um ser humano executaria o teste novamente e programa enviará 0 para o Zabbix Server.

Isso é raro acontecer, mas pode, todavia, um raio não cai duas vezes no mesmo lugar, então se o resultado por duas vezes retornar 0 ou uma latência demasiadamente alta deve ser tomada uma decisão.

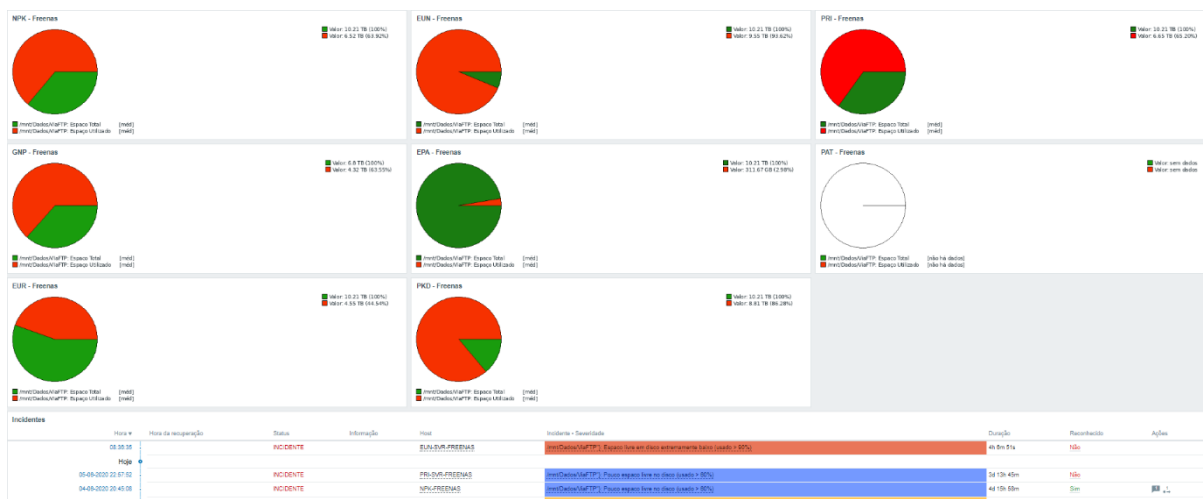
A consulta ao UDP/TCP Delay só acontece nas unidades onde se tem o equipamento de videoconferência.

3.3 DASHBOARD DEFAULT

Existem dois dashboards com o nome default entre parênteses: Freenas (default) e SonicWall (default). Estes dois mostram todos os equipamentos semelhantes do Packinggroup.

3.3.1 Freenas (default)

Este dashboard mostra todos os freenas agrupados do grupo. De modo que facilita a visualização quando se quer obter este tipo de informação. Abaixo dos vários widgets dos Freenas tem uma caixa de incidente que só mostra os incidentes dos Freenas.



3.3.2 SonicWall (default)



O dashboard SonicWall (defalt) agrupa informações sobre os Sonics, informações que temos de maneira particionada nos dashboards das unidades.

No caso temos os widgets de In/Out dos Links de cada unidade e a Disponibilidade do Link Ativo. As unidades estão separadas por linhas mas são facilmente identificadas pois suas iniciais estão no título de cada widget. Também há dois outros widgets que são os incidentes, neste dashboard mostra somente incidentes relacionados ao SonicWall, e Mapa, que mudará a cor sobre um elemento caso apresente problema para facilmente identificarmos.

Um problema recorrente foi identificado em três unidades: Prismapack, EuropackNE e Patena. Estas três ainda estão com a configuração antiga do SonicWall, então é necessário para o Zabbix Proxy ter acesso a internet e conseguir buscar e enviar informações fazer login via browser no SonicWall. Por isso caso você se depare com o gráfico de disponibilidade do link ativo desta forma, não se desespere. Antes de ligar para operadora verifique se o zabbix proxy tem conexão com a internet.



Como já explicado o gráfico de disponibilidade é uma consulta ao SpeedTest. Se o proxy não tiver conexão com internet então o script falha e retorna 0.



Junho/2020

4. DADOS RECENTES

Agora que você conhece os dashboards deve ter percebido que eles mostram um momento limitado de tempo. TCP/UDP Delay e Disponibilidade de Link Ativo mostram as últimas 2 horas, o Status e Latência Mysql e In/Out + Unidade mostram a ultima hora. Se você quiser ver um gráfico específico num período de tempo maior ou específico é nos dados recentes que você vai filtrar.

Neste exemplo quero ver o gráfico de disponibilidade de download do link principal da Norpack nas últimas 24 horas.

Primeiro passo é filtrar pelo host que obviamente se faz clicando em selecionar, no campo Host. Então aparecerá esta tela:

Se for necessário altere o grupo. No meu caso de exemplo selecionarei Rede Norpack e depois escolherei NPK-SONICWALL. Aparecerá todos os itens que é retornado via SNMP para o Zabbix Server, mas nosso objetivo concentra em encontrar os dados de disponibilidade de download nas últimas 24 horas, então procuramos pelo nome veldown.



Junho/2020

▼	NPX-SONICWALL	Performance (3 itens)				
<input type="checkbox"/>		CPU Load	09-06-2020 13:55:42	1 %	-1 %	Gráfico
<input type="checkbox"/>		RAM	09-06-2020 13:55:42	59 %		Gráfico
<input type="checkbox"/>		Simultaneous connections	09-06-2020 13:55:42	1249	-63	Gráfico
▼	NPX-SONICWALL	Status (3 itens)				
<input type="checkbox"/>		ICMP loss	09-06-2020 13:55:42	0 %		Gráfico
<input type="checkbox"/>		ICMP ping	09-06-2020 13:55:42	Up (1)		Gráfico
<input type="checkbox"/>		ICMP response time	09-06-2020 13:55:42	0.3ms		Gráfico
▼	NPX-SONICWALL	- other - (2 itens)				
<input type="checkbox"/>		veldown	09-06-2020 13:55:22	101.02 Mbps	-5.28 Mbps	Gráfico
<input type="checkbox"/>		velup	09-06-2020 13:55:22	104.71 Mbps	472.94 Kbps	Gráfico

Encontrado agora clica em gráfico. Seremos então redirecionados para este gráfico específico.

Para filtrar por horas podemos utilizar a barra:

De

ara

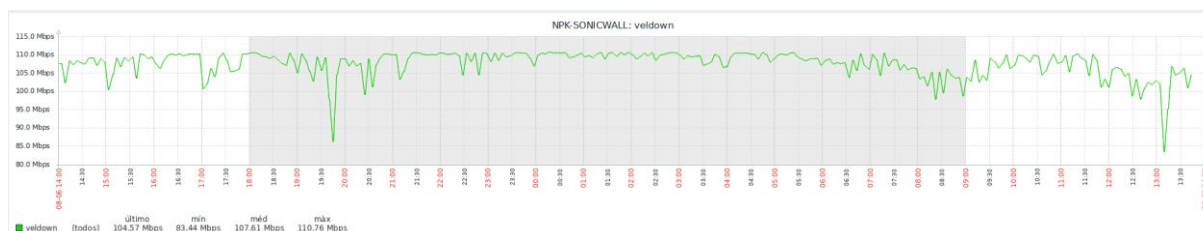
Último 2 dias
Último 7 dias
Último 30 dias
Últimos 3 meses
Últimos 6 meses
Último 1 ano
Últimos 2 anos

Ontem
Anteontem
Este dia na semana passada
Semana anterior
Mês anterior
Ano anterior

Hoje
Até agora hoje
Esta semana
Até agora nesta semana
Este mês
Até agora neste mês
Este ano
Até agora neste ano

Últimos 5 minutos
Últimos 15 minutos
Últimos 30 minutos
Última 1 hora
Últimas 3 horas
Últimas 6 horas
Últimas 12 horas

E agora temos o resultado procurado:



5. INCIDENTES

Na aba incidentes podemos filtrar por um incidente específico e exportar para CSV. Um arquivo CSV é lido pelo Excel.

Como exemplo, quero que o programa gere o relatório dos incidentes que houveram com o Link principal da Prismapack em que ele parou de responder nos últimos 3 meses.

O primeiro passo é clicarmos em Histórico e depois em aplicar.



Junho/2020

Após fazer isto aparecerá uma aba

na qual selecionaremos o tempo. Clicando então nos últimos três meses voltamos para o filtro.

Agora basta colocarmos o Host e selecionarmos também o trigger do evento. O trigger no caso que quero é Link Algar Não Responde. Ficando então assim:

Clicando em aplicar temos agora uma lista de quando e quanto tempo o link da Algar na Prismapack ficou fora.

Hora ▼	<input type="checkbox"/> Severidade	Hora da recuperação	Status	Informação	Host	Incidente	Duração
19-05-2020 14:42:20	<input type="checkbox"/> Desastre	19-05-2020 16:12:20	RESOLVIDO		PRI-SONICWALL	Link Algar Não Responde	1h 30m
19-05-2020 11:09:20	<input type="checkbox"/> Desastre	19-05-2020 14:34:20	RESOLVIDO		PRI-SONICWALL	Link Algar Não Responde	3h 25m
19-05-2020 09:52:20	<input type="checkbox"/> Desastre	19-05-2020 10:51:20	RESOLVIDO		PRI-SONICWALL	Link Algar Não Responde	59m
19-05-2020 08:35:20	<input type="checkbox"/> Desastre	19-05-2020 09:28:20	RESOLVIDO		PRI-SONICWALL	Link Algar Não Responde	53m
19-05-2020 07:57:20	<input type="checkbox"/> Desastre	19-05-2020 08:07:20	RESOLVIDO		PRI-SONICWALL	Link Algar Não Responde	10m
19-05-2020 07:45:20	<input type="checkbox"/> Desastre	19-05-2020 07:48:20	RESOLVIDO		PRI-SONICWALL	Link Algar Não Responde	3m
Maio							
24-04-2020 14:06:20	<input type="checkbox"/> Desastre	24-04-2020 14:11:46	RESOLVIDO		PRI-SONICWALL	Link Algar Não Responde	5m 26s
23-04-2020 17:13:20	<input type="checkbox"/> Desastre	23-04-2020 17:14:20	RESOLVIDO		PRI-SONICWALL	Link Algar Não Responde	1m
23-04-2020 17:02:20	<input type="checkbox"/> Desastre	23-04-2020 17:06:46	RESOLVIDO		PRI-SONICWALL	Link Algar Não Responde	4m 26s
23-04-2020 16:04:20	<input type="checkbox"/> Desastre	23-04-2020 16:41:20	RESOLVIDO		PRI-SONICWALL	Link Algar Não Responde	37m
23-04-2020 15:03:20	<input type="checkbox"/> Desastre	23-04-2020 15:45:20	RESOLVIDO		PRI-SONICWALL	Link Algar Não Responde	42m



Junho/2020

Por fim basta clicar em Exportar para CSV. Após abrir o documento no Excel salve no formato Pasta de Trabalho Excel, depois abra uma nova planilha clique em dados > importar CSV e teremos o arquivo importado em XLS.

Hora	Hora da recupera	Status	Host	Incidente	Operational data
19/05/2020 14:42	19/05/2020 16:12	RESOLVIDO	PRI-SONICWALL	Link Algar Não Responde	1h 30m
19/05/2020 11:09	19/05/2020 14:34	RESOLVIDO	PRI-SONICWALL	Link Algar Não Responde	3h 25m
19/05/2020 09:52	19/05/2020 10:51	RESOLVIDO	PRI-SONICWALL	Link Algar Não Responde	59m
19/05/2020 08:35	19/05/2020 09:28	RESOLVIDO	PRI-SONICWALL	Link Algar Não Responde	53m
19/05/2020 07:57	19/05/2020 08:07	RESOLVIDO	PRI-SONICWALL	Link Algar Não Responde	10m
19/05/2020 07:45	19/05/2020 07:48	RESOLVIDO	PRI-SONICWALL	Link Algar Não Responde	3m
24/04/2020 14:06	24/04/2020 14:11	RESOLVIDO	PRI-SONICWALL	Link Algar Não Responde	5m 26s
23/04/2020 17:13	23/04/2020 17:14	RESOLVIDO	PRI-SONICWALL	Link Algar Não Responde	1m
23/04/2020 17:02	23/04/2020 17:06	RESOLVIDO	PRI-SONICWALL	Link Algar Não Responde	4m 26s
23/04/2020 16:04	23/04/2020 16:41	RESOLVIDO	PRI-SONICWALL	Link Algar Não Responde	37m
23/04/2020 15:03	23/04/2020 15:45	RESOLVIDO	PRI-SONICWALL	Link Algar Não Responde	42m



Junho/2020