JOÃO PESSOA-PB

OUT/2013

Histórico de Atualizações

Data	Versão	Responsável	Alterações
16 ago 2012	1.0	Aécio Pires	Versão inicial
24 out 2012	1.1	Aécio Pires	Ajuste na documentação
18 jun 2013	1.2	Aécio Pires	Atualização para usar o Zabbix 2.0.6
18 out 2013	1.3	Aécio Pires	Atualização para usar o Zabbix 2.0.9

Aécio dos Santos Pires

http://aeciopires.com
aeciopires@gmail.com

Especialista em Segurança da Informação – iDEZ, tecnólogo em Redes de Computadores – IFPB, administrador de sistemas da Dynavídeo e membro da comunidade Zabbix Brasil.

Licença de Uso

Sumário

1. Introdução

Zabbix é um sistema web, gratuito e de código aberto usado para o monitoramento e gerenciamento de equipamentos de rede (câmera de segurança, roteador, computador, etc) criado por Alexei Vladishev e, atualmente, desenvolvido pela Zabbix SIA.

Ele monitora vários parâmetros de rede e checa a integridade dos equipamentos, usando um mecanismo de notificação flexível que permite aos usuários configurarem o envio de alertas por e-mail, SMS ou Jabber. Esta característica permite uma rápida reação aos problemas que forem detectados.

O Zabbix é composto de vários componentes de software, os principais são:

- **Zabbix Server**: é o componente central do sistema. Ele pode verificar remotamente os serviços de rede (como serviço web e e-mail), utilizando a checagem simples, mas também é o componente central para que os agentes enviem informações e estatísticas a cerca da disponibilidade e integridade do equipamento que está sendo monitorado. Depois que o servidor recebe essas informações, ele processa, gerencia os equipamentos, exibe relatórios, envia alertas e toma ações dependendo da configuração.
- **Banco de dados:** é onde os dados, as informações e configurações são armazenadas. O banco de dados pode ser acessado diretamente pelo Zabbix server e pela interface Web. O Zabbix tem suporte aos bancos de dados: PostgreSQL, MySQL, Oracle, SQLite e DB2 da IBM.
- **Interface web**: é por ela que o Zabbix pode ser configurado e as informações visualizadas.
- **Agente Zabbix**: aplicação cliente do Zabbix que coleta informações do equipamento e envia ao servidor. O agente é capaz de acompanhar ativamente o uso dos recursos e aplicações locais, tais como: discos rígidos, memória, processador, processos, serviços e aplicativos em execução.
- **Zabbix Proxy**: é uma parte opcional do Zabbix. O Proxy coleta dados de desempenho e disponibilidade, em nome de um servidor Zabbix com a vantagem de coletar milhares de informações por segundo, utilizando um hardware modesto. Podemos considerá-lo como um super agente.
- **Java Gateway**: O Zabbix 2.0 trouxe o suporte nativo ao monitoramento de aplicações JMX através do daemon **Zabbix Java gateway**. Quando o servidor Zabbix quer saber o valor de um contador de JMX de um host, ele pede a esse daemon, que usa a API de gerenciamento JMX para consultar a aplicação remotamente.

Neste tutorial será ensinado como monitorar o desempenho do Glassfish 2.1 usando o Zabbix. É assumido que você já tem o servidor Zabbix e/ou Zabbix proxy instalado e que possa acessar a máquina que possui o Glassfish. Se você ainda não instalou o Zabbix, pode instalar usando algum dos tutoriais na página http://zabbixbrasil.org/?p=272.

Para a elaboração deste tutorial foram utilizados os seguintes cenários:

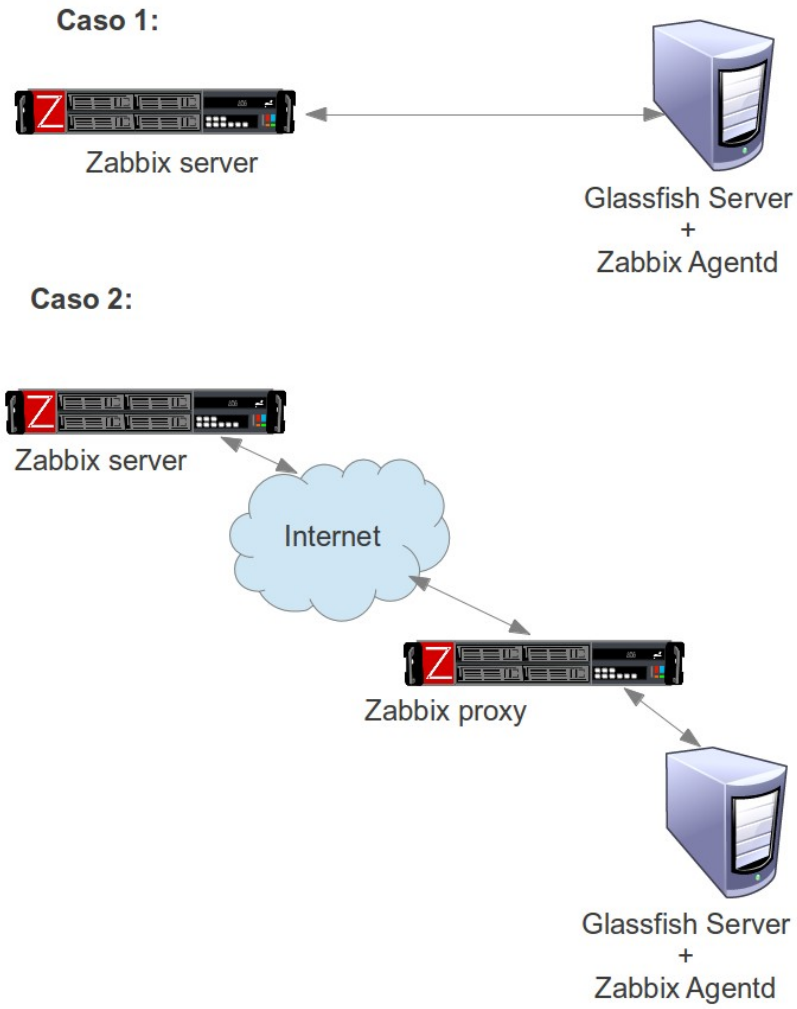
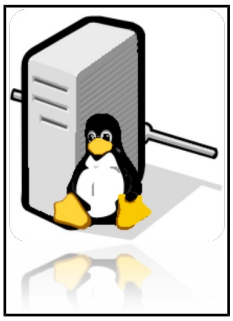


Figura 1: Cenários de monitoramento do Glassfish.

As máquinas utilizadas neste tutorial possuem a seguinte configuração.



Processador: Intel Dual Core 1.8 GHz

Memoria RAM: 2 GB

HD: 10 GB

Sistema operacional: Ubuntu Desktop 12.04 32 bits.

2. Configurando o Zabbix 2.0 para monitorar aplicações Java

Para monitorar aplicações Java, o servidor Zabbix ou o Zabbix Proxy precisa ser compilado com a opção **--enable-java**. Os tutoriais abaixo ensinam a instalar o Zabbix com essa opção.

Zabbix Server 2.0 usando PostgreSQL no Ubuntu:
http://zabbixbrasil.org/files/Tutorial_de_instalacao_do_Zabbix_2.0.0.pdf

Zabbix Server 2.0 usando MySQL no Debian:
http://zabbixbrasil.org/files/Tutorial_de_instala%C3%A7%C3%A3o_do_Zabbix_2.0.0_debian.pdf

Zabbix Proxy 2.0 usando SQLite no Ubuntu:
http://zabbixbrasil.org/files/Tutorial_de_instalacao_do_Zabbix_Proxy_2.0.0.pdf

OBS.: Para o Java Gateway funcionar é preciso ter o Java instalado na mesma máquina que está executando o servidor Zabbix ou o Zabbix Proxy. O Java pode ser verificado com o comando "**java -version**".

Para ter certeza que o Java Gateway foi compilado com sucesso na instalação do Zabbix server ou Zabbix proxy, verifique se o diretório **/usr/local/sbin/zabbix_java/** foi criado. Se sim, o conteúdo desse diretório pode ser verificado com os seguintes comandos.

```
$ sudo apt-get install tree
$ tree /usr/local/sbin/zabbix_java/
├── bin
│   └── zabbix-java-gateway-2.0.9.jar
├── lib
│   ├── logback-classic-0.9.27.jar
│   ├── logback-console.xml
│   ├── logback-core-0.9.27.jar
│   ├── logback.xml
│   ├── org-json-2010-12-28.jar
│   └── slf4j-api-1.6.1.jar
├── settings.sh
├── shutdown.sh
└── startup.sh
```

Para que o monitoramento JMX funcione, o serviço do Zabbix Java Gateway tem que estar em execução. Execute o script **startup.sh** encontrado no diretório /usr/local/sbin/zabbix_java/ .

```
$ sudo /usr/local/sbin/zabbix_java/startup.sh
```

Para saber se o serviço está em execução, pode ser usado um dos comandos abaixo:

```
$ sudo ps aux | grep zabbix_java
root     16434  0.2  0.2 5874628 41212 ?       Sl   18:22   0:01 java -server
-classpath lib:lib/logback-classic-0.9.27.jar:lib/logback-core-0.9.27.jar:lib/org-json-
2010-12-28.jar:lib/slf4j-api-1.6.1.jar:bin/zabbix-java-gateway-2.0.6.jar
-Dzabbix.pidFile=/tmp/zabbix_java.pid com.zabbix.gateway.JavaGateway
root     30555  0.0  0.0  13588   920 pts/1    S+   18:37   0:00 grep --color=auto
zabbix_java
```

ou:

```
$ sudo apt-get install nmap
$ sudo nmap -p 10052 localhost
Starting Nmap 5.00 ( http://nmap.org ) at 2012-10-24 10:46 BRST
Warning: Hostname localhost resolves to 2 IPs. Using 127.0.0.1.
Interesting ports on localhost (127.0.0.1):
PORT      STATE SERVICE
10052/tcp open  unknown
```

Crie o usuário **zabbix** no sistema operacional com os comandos abaixo.

```
$ sudo adduser zabbix
$ sudo adduser zabbix admin
```

Digite o comando **visudo** e no arquivo a ser aberto adicione a linha abaixo para que o usuário zabbix seja capaz de usar o comando **sudo** sem informar a senha durante a execução de comandos para monitorar o Glassfishv2.

```
zabbix ALL=(ALL) NOPASSWD: ALL
```

Em seguida, salve o arquivo.

Os arquivos de configuração do Zabbix 2.0 ficam em **/usr/local/etc**.

Edite o arquivo **/usr/local/etc/zabbix_server.conf** (se o servidor Zabbix estiver instalado na mesma rede do servidor Glassfish) ou edite o arquivo **/usr/local/etc/zabbix_proxy.conf** (se o Zabbix Proxy estiver instalado na mesma rede do servidor Glassfish) e altere apenas os seguintes parâmetros informando os valores semelhantes aos do exemplo abaixo:

```
JavaGateway=<ip_servidor_glassfish>
JavaGatewayPort=10052
StartJavaPollers=5
```

Depois reinicie o serviço.

```
$ sudo /etc/init.d/zabbix-server stop
$ sudo /etc/init.d/zabbix-server start
```

Ou:

```
$ sudo /etc/init.d/zabbix-proxy stop
$ sudo /etc/init.d/zabbix-proxy start
```

OBS.: Se o servidor Zabbix e/ou Proxy estiverem atrás de um firewall que faz uso do NAT, é preciso configurar o redirecionamento de pacotes na porta 10052/TCP.

2.1. Scripts de inicialização do Java Gateway

Coloque o Zabbix Java Gateway para iniciar automaticamente, no boot do sistema operacional, criando o script abaixo.

====> Crie arquivo **/etc/init.d/zabbix-java** e adicione o conteúdo abaixo.

```
#!/bin/sh

NAME=zabbix-java
PATH=/bin:/usr/bin:/sbin:/usr/sbin:/home/zabbix/bin
DAEMON=/usr/local/sbin/zabbix_java/startup.sh
DOWN=/usr/local/sbin/zabbix_java/shutdown.sh
DESC="Zabbix Java Gateway daemon"
PID=/tmp/zabbix_java.pid

test -f $DAEMON || exit 0

set -e

case "$1" in
  start)
        echo "Starting $DESC"
        $DAEMON
        ;;
  stop)
        echo "Stopping $DESC"
        $DOWN
        ;;
  *)
        N=/etc/init.d/$NAME
        # echo "Usage: $N {start|stop}" >&2
        echo "Usage: $N {start|stop}" >&2
        exit 1
        ;;
esac
exit 0
```

Torne o arquivo executável com o comando abaixo.

```
$ sudo chmod +x /etc/init.d/zabbix-java
```

Em seguida, execute o script:

```
$ sudo /etc/init.d/zabbix-java start
```

Habilite o script para ser executado quando o computador for ligado.

```
$ sudo update-rc.d -f zabbix-java defaults
```

3. Configurando o Glassfish2.1

Edite o arquivo de configuração do Glassfishv2 que fica em **PATH_GLASSFISH/domain/domain1/config/domain.xml**

OBS.: Substitua PATH_GLASSFISH pelo diretório em que está instalado o Glassfish (Ex.: /usr/share/glassfishv2).

Neste arquivo localize a seção **<java-config>** e dentro dela adicione as seguintes linhas:

```
<jvm-options>-Dcom.sun.management.jmxremote.authenticate=false</jvm-options>
<jvm-options>-Dcom.sun.management.jmxremote.ssl=false</jvm-options>
```

Localize também a porta **8686** e altere o **<jmx-connector>** referente a porta 8686 conforme mostrado no exemplo abaixo:

Antes:

```
<jmx-connector accept-all="false" address="0.0.0.0" auth-realm-name="admin-realm" enabled="true" name="system" port="8686" protocol="rmi_jrmp" security-enabled="false">
        <ssl cert-nickname="s1as" client-auth-enabled="false" ssl2-enabled="false" ssl3-enabled="true" tls-enabled="true" tls-rollback-enabled="true"/>
      </jmx-connector>
```

Depois:

```
<jmx-connector accept-all="true" address="0.0.0.0" auth-realm-name="admin-realm" enabled="true" name="system" port="12345" protocol="rmi_jrmp" security-enabled="false">
        <ssl cert-nickname="s1as" client-auth-enabled="false" ssl2-enabled="false" ssl3-enabled="true" tls-enabled="true" tls-rollback-enabled="true"/>
</jmx-connector>
```

Localize também a seção **<monitoring-service>** e altere conforme o exemplo abaixo:

Antes:

```
<monitoring-service>
        <module-monitoring-levels connector-connection-pool="OFF" connector-service="OFF" ejb-container="OFF" http-service="OFF" jdbc-connection-pool="OFF" jms-service="OFF" jvm="OFF" orb="OFF" thread-pool="OFF" transaction-service="OFF" web-container="OFF"/>
    </monitoring-service>
```

Depois:

```
<monitoring-service>
        <module-monitoring-levels connector-connection-pool="OFF" connector-service="OFF" ejb-container="OFF" http-service="LOW" jdbc-connection-pool="HIGH" jms-service="OFF" jvm="OFF" orb="OFF" thread-pool="OFF" transaction-service="OFF" web-container="OFF"/>
    </monitoring-service>
```

Depois disso reinicie o Glassfish com os comandos abaixo.

```
$ sudo PATH_GLASSFISH/bin/asadmin stop-domain
$ sudo PATH_GLASSFISH/bin/asadmin start-domain domain1
Starting Domain domain1, please wait.
Default Log location is ../glassfish/domains/domain1/logs/server.log.
Redirecting output to ../glassfish/domains/domain1/logs/server.log
Domain domain1 is ready to receive client requests. Additional services are being started in background.
Domain [domain1] is running [Sun GlassFish Enterprise Server v2.1.1 ((v2.1 Patch06)(9.1_02 Patch12)) (build b31g-fcs)] with its configuration and logs at: [../glassfish/domains].
Admin Console is available at [http://localhost:4848].
Use the same port [4848] for "asadmin" commands.
User web applications are available at these URLs:
[http://localhost:8080 https://localhost:8181].
Following web-contexts are available:
[/web1 /__wstx-services ].
Standard JMX Clients (like JConsole) can connect to JMXServiceURL:
[service:jmx:rmi:///jndi/rmi://xxx:12345/jmxrmi] for domain management purposes.
Domain listens on at least following ports for connections:
[8080 8181 4848 3700 3820 3920 12345].-> olha aqui a porta aberta.
```

Verificando se o Glassfish está recebendo conexões na porta 12345.

```
$ sudo nmap -p 12345 localhost
Starting Nmap 5.21 (http://nmap.org) at 2012-07-04 09:36 BRT
Nmap scan report for localhost (127.0.0.1)
```

```
Host is up (0.000063s latency).
rDNS record for 127.0.0.1: localhost.localdomain
PORT          STATE SERVICE
12345/tcp open netbus
```

4. Cadastrando o Zabbix Java na interface web do Zabbix

Para o Zabbix monitorar o Glassfish será preciso que você se lembre do usuário e senha usada para acessar o painel de administração Web do Glassfish como na URL http://localhost:4848. Por padrão, o usuário é **admin**, e a senha é **adminadmin**.

No Zabbix, acesse o menu **Configuração (Configuration)** > **Hosts** e, em seguida, clique no botão **Criar Host (Create Host)**. Cadastre o host cliente como mostrado nas Figura 2.

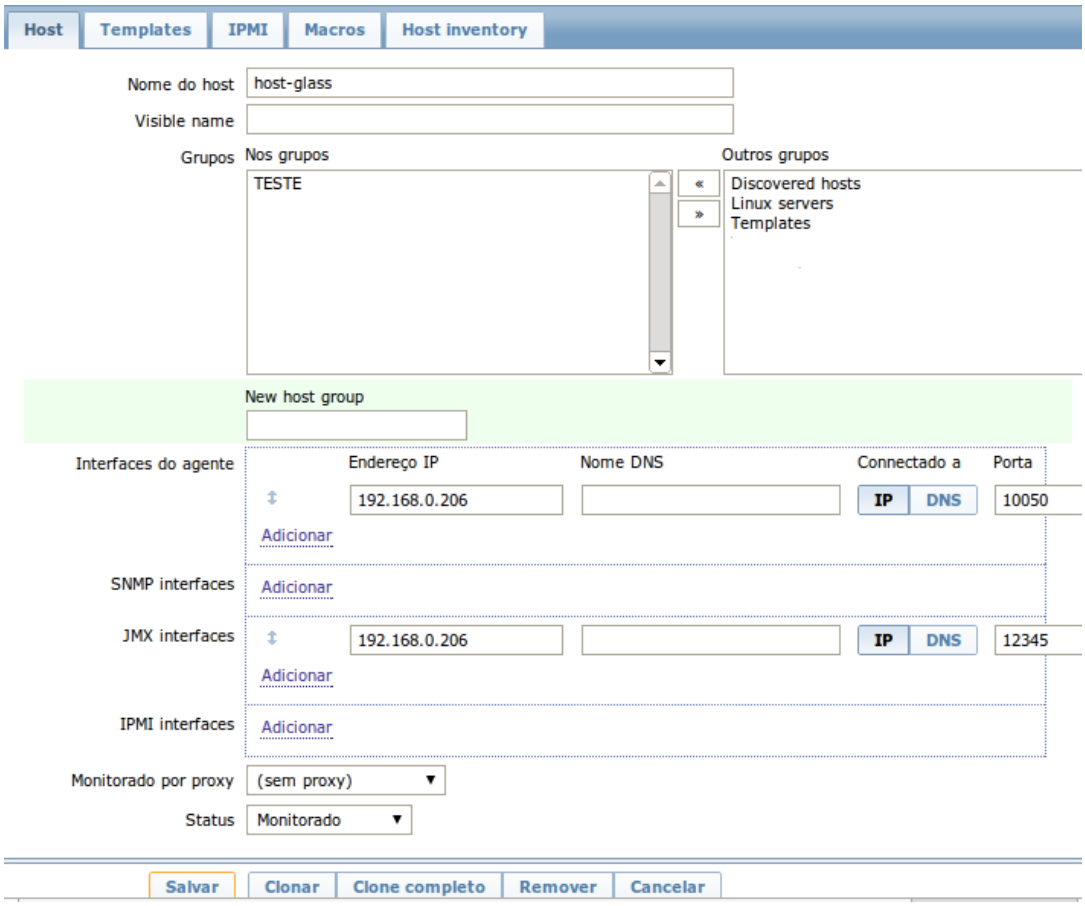


Figura 2: Cadastrando o host cliente.

OBS.: No campo **Host Name** deve ser informado o nome do servidor do Glassfish conforme configurado no parâmetro **Hostname** do arquivo **/usr/local/etc/zabbix_agentd.conf**.

Baixe os UserParameters customizados para monitorar o Glassfishv2 em: http://zabbixbrasil.org/files/UserParameters_Glassfish2-1.txt

Copie esse arquivo para a máquina que possui o servidor Glassfish.

Execute o comando abaixo para colocar os UserParameters dentro do arquivo de configuração do Zabbix Agentd instalado nessa máquina.

```
$ sudo cat UserParameters_Glassfish2-1.txt >> /usr/local/etc/zabbix_agentd.conf
$ sudo /etc/init.d/zabbix-agentd stop
$ sudo /etc/init.d/zabbix-agentd start
```

Baixe o template de monitoramento do Glassfish2.1 em http://zabbixbrasil.org/files/glassfishv2_template.xml .

Importe o template para o Zabbix acessando o menu **Configuração (Configuration)** > **Templates** e, em seguida, clique no botão **Importar.** Selecione o template e deixe todas as opções padrão. Ao final clique no botão **Importar.**

Acesse novamente o menu **Configuração (Configuration)** > **Templates** e, em seguida clique em **itens** ao lado do template **Glassfish2.1_TESTE.** Selecione todos os itens e no final da página escolha a opção **Atualização em massa**, conforme mostrado na Figura 3.

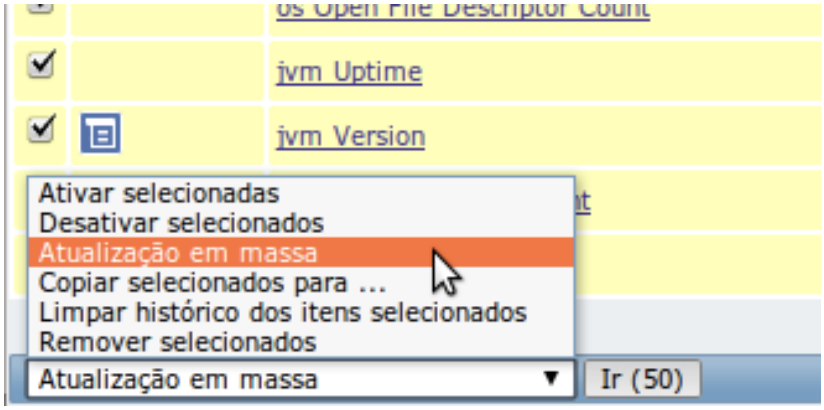


Figura 3: Atualização em massa.

Informe o usuário e senha de acesso ao painel administrativo do Glassfish e clique no botão **Atualizar,** conforme mostrado na Figura 4**.**

Figura 4: Atualização em massa do usuário e senha.

Agora atribua este template ao host e visualize os dados do monitoramento no menu **Monitoramento (Monitoring) > Gráficos (Graphs)**.

4. Considerações finais

Neste tutorial foi mostrado como monitorar o Glassfish2.1 usando o Zabbix Proxy e o Zabbix Server.

Na página http://zabbixbrasil.org/?page_id=7 você pode encontrar outros tutoriais.

Abraço e que Deus o(a) abençoe. Leia o Salmo 55:22. Jesus é bom, te ama e quer salvar tua alma. :-)

5. Referências

[1] Java Gateway. Disponível em: http://www.zabbix.com/documentation/2.0/manual/concepts/java Acessado em: 21 de outubro de 2013.

[2] JMX Monitoring. Disponível em: http://www.zabbix.com/documentation/2.0/manual/config/items/itemtypes/jmx_monitoring Acessado em: 21 de outubro de 2013.

[3] LIMA, Janssen. Monitorando o JBoss no Zabbix. Disponível em: http://janssenlima.blogspot.com/2012/07/monitorando-servidor-jboss-no-zabbix.html Acessado em: 21 de outubro de 2013.