

Configuração SNMP Trap no Zabbix

1 INSTALAÇÃO DE PRÉ-REQUISITOS

Para que o Zabbix possa receber traps enviadas pelos hosts é necessário instalar alguns pacotes e módulos na máquina do Zabbix. Acesse <http://sourceforge.net/projects/snmpptt/> e faça o download do pacote SNMPTT (SNMP Trap Translator).

Depois acesse <http://snmpptt.sourceforge.net/docs/snmpptt.shtml> e instale todos os requisitos da seção "Requirements". Verifique se todos os pacotes e módulos necessários foram instalados corretamente, isso é essencial.

2 INSTALAÇÃO DO SNMPTT

Na pasta pacote SNMPTT baixado você irá encontrar os seguintes arquivos:

snmpptt

snmpptthandler-embedded

snmpptt.ini

snmpptt.conf.generic (na pasta /examples)

snmpptt-init.d

snmpptt.logrotate

Vamos copiar esses arquivos para a pasta **/etc/snmp** e editá-los conforme descrito a seguir:

- 1) Certifique-se de que o snmptrapd tem incorporado o suporte Perl habilitado. Ao compilar a partir dos fontes, utilize a opção de configuração - 'enable-embedded-perl'.

Faça no terminal **snmptrapd-H 2> & 1 | grep perl**. O resultado deve ser **PERLCODE perl** se o Perl embutido estiver habilitado.

Se não estiver disponível, você precisa compilar Net-SNMP usando o - **enable-embedded-perl** NA opção de configuração.

- 2) Copie **snmpptt** para **/usr/sbin/** e garanta que ele é executável (**chmod +x snmpptt**)
- 3) Copie **snmpptthandler-embedded** para **/usr/sbin/**. Ele não precisa ser executável, como é chamado diretamente pelo snmptrapd.
- 4) Copie **snmpptt.ini** para **/etc/snmp/** e edite as opções dentro do arquivo.

Você deverá colocar o caminho do seu arquivo snmptt.conf. Por exemplo:

```
snmptt_conf_files = <<END
/etc/snmp/snmptt.conf
END
```

- 5) Copie **snmptt.conf.generic** para **/ etc / snmp** (renomeie o arquivo durante a cópia para snmptt.conf) ou use o comando touch para criar o arquivo (**touch / etc / snmp / snmptt.conf**).
- 6) Crie a pasta de log **/ var / log / snmptt /**
mkdir /var/log/snmptt/
- 7) Crie o arquivo **snmptrapd.conf** na pasta **/etc/snmp** com as seguintes linhas:

traphandle default snmptt

disableAuthorization yes

authCommunity log, execute, net public

outputOption n
- 8) Crie a pasta de spool **/ var / spool / snmptt /**
mkdir /var/spool/snmptt/
- 9) Um script de inicialização está incluído na pasta de download do SNMPTT, que pode ser usado para iniciar e parar **snmptt** em Mandrake, RedHat e outros sistemas.

Copie o script **snmptt-init.d** para o diretório **/ etc / rc.d / init.d / snmptt**
- 10) Adicione o serviço usando **chkconfig** :
chkconfig - add snmptt
- 11) Configure o serviço para iniciar em nível 2345 de execução:
chkconfig - level 2345 snmptt on
- 12) Snmptt será iniciada na próxima reinicialização, ou pode ser iniciado imediatamente com:
service snmptt start
ou
/ etc / rc.d / init.d / snmptt start

Para iniciar manualmente snmptt, use:

snmptt – daemon

- 13) Um script de rotação de log está incluído, que pode ser usado para rodar os arquivos de log em Mandrake, RedHat e outros sistemas.

Copie o arquivo **snmptt.logrotate.d** para **/etc/logrotate.d** (renomeie o arquivo para **snmptt** durante a cópia):

cp snmptt.logrotate / etc / logrotate.d / snmptt

Edite o **/ etc / logrotate.d / snmptt** e atualize os caminhos e frequência de rotação, conforme necessário.

- 14) Inicie o **snmptrapd** usando a linha de comando: **snmptrapd -On** .

3 CONFIGURAÇÕES

- 1) Edite o arquivo **snmptt.ini**

log_enable = 1

log_file= /var/snmptrap/zabbix_traps.tmp

(coloque aqui o caminho que você desejar para salvar o arquivo de traps que vai ser gerado)

date_time_format = %H:%M:%S %Y/%m/%

- 2) Edite o arquivo **zabbix_server.conf**

StartSNMPTrapper=1

SNMPTrapperFile= /var/snmptrap/zabbix_traps.tmp

- 3) Edite o arquivo **snmptt.conf**

Acrescente as seguintes linhas:

EVENT general .* "General event" Normal

FORMAT ZBXTRAP \$aA \$ar

Essa configuração permitirá que o Zabbix capture traps de qualquer OID (.*) através de um item que tiver a chave snmptrap ["General Event"].

4 CONFIGURAÇÃO NO ZABBIX

- 1) Adicione o Zabbix o host que você deseja capturar as traps. Adicione uma SNMP interface com o IP do host e com a porta 162.
- 2) Crie um item para o host com a seguinte configuração:
Name: Teste_snmptrap
Type: SNMP trap
Key: snmptrap ["General event"]
Host interface: IP do host:162
Type of information: Log
Log time format: hh:mm:ss yyyy/MM/dd
- 3) Para fazer um teste crie o item acima no próprio host Zabbix Server (IP = 127.0.0.1) e envie uma trap do Zabbix para ele mesmo:

```
snmptrap -v 1 -c public 127.0.0.1 '.1.3.6.1.6.3.1.1.5.3' '0.0.0.0' 6 33  
'55' .1.3.6.1.6.3.1.1.5.3 s "teststring000"
```

No arquivo gerado **zabbix_traps** deverá aparecer a seguinte linha:

```
15:48:18 2011/07/26 .1.3.6.1.6.3.1.1.5.3.0.33 Normal "General event"  
localhost - ZBXTRAP 127.0.0.1 127.0.0.1
```

Verifique no Zabbix em **Monitoring->Latest Data** se o item coletou as informações da trap recebida para o host Zabbix Server.

- 4) Para criar itens com traps específicas edite o arquivo snmpptt.conf colocando o OID e tipo de trap. Por exemplo:

```
EVENT [nome do evento] [OID do evento] ["Categoria"] [Severidade]  
FORMAT ZBXTRAP $aA $ar [descrição da trap]
```

No item do Zabbix use a seguinte chave:

```
Key: snmptrap ["Categoria"]
```

Dessa forma esse item irá coletar as traps recebidas apenas com essa categoria. Assim é possível criar um item para cada tipo de trap associada a um OID diferente, possibilitando a criação de triggers específicas para cada tipo de trap recebida.

Uma boa prática é colocar o nome do evento como o nome do identificador OID. Para isso você pode utilizar o comando **snmptranslate** e traduzir o OID numérico para a forma textual.(<http://rodrigo.lncc.br/index.php/Snmptranslate>)

É possível modificar o formato que as traps são armazenadas no arquivo modificando o que vem depois de FORMAT ZBXTRAP. Para alterar isso consulte a referência [3] e modifique conforme sua preferência.

5 REFERÊNCIAS

[1] <https://www.zabbix.com/documentation/2.0/manual/config/items/itemtypes/snmptrap>

[2] <http://snmptt.sourceforge.net/docs/snmptt.shtml#Installation-Unix>

[3] <http://www.snmptt.org/docs/snmptt.shtml#SNMPTT.CONF-Configuration-file-format>

Acessado em 20/03/2014

Tutorial feito em 28/03/2014 utilizando o Zabbix 2.2.2 e distribuição CentOS.

Contato:

Thayane Viana

Graduanda em Engenharia de Redes de Comunicação – UnB

E-mail: thayaneviana@hotmail.com

*Filho meu, se aceitares as minhas palavras, e esconderes contigo os meus mandamentos,
Para fazeres o teu ouvido atento à sabedoria; e inclinares o teu coração ao entendimento;
Se clamares por conhecimento, e por inteligência alçares a tua voz,
Se como a prata a buscares e como a tesouros escondidos a procuraes,
Então entenderás o temor do Senhor, e acharás o conhecimento de Deus.
Porque o Senhor dá a sabedoria; da sua boca é que vem o conhecimento e o entendimento. (Pv 2:1-6)*