

Configuración y captura de trazas de red en XenServer

Escrito por cristiansan

Martes, 13 de Abril de 2010 16:48 - Actualizado Martes, 13 de Abril de 2010 16:54

En esta ocasión mostramos como configurar y capturar una traza de red en XenServer, toda la configuración la realizaremos a nivel de línea de comando CLI.

Conectamos vía ssh en nuestro servidor.

Primero vamos a identificar la red dónde realizar la traza

```
$ xe pif-list
```

Ello indicará una lista de nuestros dispositivos, si queremos indicar la información que queremos que nos muestre lo haremos con el parámetro "params="

```
$ xe pif-list params=device,network-uuid
```

Ello nos mostrará una lista de los dispositivos de red indicando unicamente el dispositivo y el uuid de red.

Una vez conocemos el dispositivo dónde realizar la traza, utilizaremos la herramienta tcpdump para la captura del trafico y la rediregiremos a un fichero que posteriormente podremos analizar. Para ello:

```
$ tcpdump -npi <dispositivo> > /path/<fichero donde guardaremos la traza>.
```

Ejemplo:

Configuración y captura de trazas de red en XenServer

Escrito por cristiansan

Martes, 13 de Abril de 2010 16:48 - Actualizado Martes, 13 de Abril de 2010 16:54

```
[root@xenserver01 ~]# tcpdump -i eth0 > /var/prueba.log
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
```

Cortaremos la captura de paquetes mediante la combinación de teclas “Control + C”.

```
8293 packets captured
16590 packets received by filter
0 packets dropped by kernel
```

Vamos ahora a realizar una traza sobre nuestro virtual bridge. Para ello utilizaremos el mismo procedimiento, primero localizamos el interface y su uuid (necesario para localizar posteriormente la virtual Bridge).

```
$ xe pif-list params=device,network-uuid
```

Localizado el uuid, procedemos a localizar el Bridge asociado a nuestro interface de red.

```
$ xe network-list uuid=<uuid localizado> params=bridge,name-label
```

Ejemplo:

```
[root@xenserver01 ~]# xe network-list uuid=7a193686-4d7b-a09c-c19b-39c53d1ef6ba
params=bridge,name-label
name-label ( RW) : Pool-wide network associated with eth0
bridge ( RO): xenbr0
```

Configuración y captura de trazas de red en XenServer

Escrito por cristiansan

Martes, 13 de Abril de 2010 16:48 - Actualizado Martes, 13 de Abril de 2010 16:54

Localizado el interface, procedemos igual que antes con tcpdump.

```
$ tcpdump -npi xenbr0 > /var/log2
```

Salimos con Cntrl+C y ya podemos revisar nuestra traza.

Podemos realizar el mismo procedimiento para realizar una traza sobre el dispositivo de red de una VM corriendo en nuestro de XenServer. Para ello, siguiendo como hasta ahora....

Identificamos el dom-Id de nuestra máquina virtual:

```
$ xe vm-list name-label=vDCTEST params=dom-id
```

```
dom-id ( RO) : 40
```

Localizado el DOM-ID procedemos a localizar el dispositivo VIF de nuestra VM.

```
$ xe vif-list vm-name-label=vDCTEST params=device  
device (RO) : 0
```

Con estos datos ya podemos lanzar la traza, la sintaxis para TCPDUMP seria:

Configuración y captura de trazas de red en XenServer

Escrito por cristiansan

Martes, 13 de Abril de 2010 16:48 - Actualizado Martes, 13 de Abril de 2010 16:54

```
$ tcpdump -npi vif<DOM-ID>.<DEVICE>
```

En nuestro caso quedaria:

```
$ tcpdump -npi vif40.0 > /var/trazavm.log
```

Cortamos el registro con control+c.